|  |
| --- |
| IU |
| Standards der Informationssicherheit |
| Kurscode |

# Übergeordnete Lernziele

In der heutigen Zeit ist die Abhängigkeit vom Internet und der Vernetzung unserer Welt allgegenwärtig. Die Verbreitung von Social-Media-Plattformen, Tools und interaktiven Technologien nimmt zu. Dies führt zu einer Zunahme von digitalen Fußabdrücken und anderen Nachverfolgungsmethoden der Nutzer:innen. Diese reichen von einfachen Hacking- oder technischen Ansätzen bis hin zu subtilen, sozialen und nicht-technischen Strategien wie Social Engineering, die den menschlichen Geist nutzen und manipulieren. Nahezu alle Aspekte des Lebens und der Interaktion verlagern sich in das Online-Universum, was sowohl für Einzelpersonen als auch für Organisationen erhebliche Sicherheitsbedenken mit sich bringt. Die Sicherung von Informationsbeständen, die organisiertes, verwaltetes und wertvolles Wissen oder Daten darstellen, wird häufig vernachlässigt, obwohl dies sehr kostspielig sein kann.

Dieser Kurs bietet eine Navigationshilfe durch die komplexe Landschaft der Informationssicherheit, einschließlich der damit verbundenen rechtlichen und regulatorischen Anforderungen sowie aller relevanten Normen und Standards, die zum Schutz der Organisationsressourcen umgesetzt werden müssen. Die meisten Organisationen konzentrieren sich auf den Aufbau von IT-Systemen und vernachlässigen dabei den übergeordneten Managementkontext. Dieser umfasst Normen und Standards, die Organisationen dabei unterstützen, ihre Prozesse und Abläufe nach Best Practices und globalen Methoden für das Informationssicherheitsmanagement auszurichten. Die Internationale Organisation für Normung (ISO) ist für die Überprüfung, Verbesserung und Aktualisierung dieser Normen zuständig.

Der Kurs vermittelt zunächst grundlegende Sicherheitskonzepte und Terminologie. Anschließend konzentriert er sich auf das umfassende Informationssicherheits-Framework, das in einer Organisation umgesetzt werden muss – insbesondere ein Informationssicherheitsmanagementsystem (ISMS). Sie lernen, wie ein ISMS initiiert wird und wie die Prozesse während und nach der Implementierung umgesetzt, verwaltet und überwacht werden.

# Lektion 1 – Einführung in die Informationssicherheit

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… kennen Sie grundlegende Sicherheitsbegriffe, Konzepte und Ziele der Informationssicherheit.

… kennen Sie Informationssicherheitsstandards und rechtliche Rahmenbedingungen und können diese beschreiben.

… sind Sie in der Lage, Informationssicherheitsstandards, wie die ISO 27000-Reihe und die BSI-Standards zu erläutern.

… können Sie Informationssicherheitsmanagementsysteme (ISMS) entwickeln, ihre Feinheiten, einschließlich Maßnahmen und Verfahren, analysieren sowie Maßnahmen zur kontinuierlichen Verbesserung solcher Systeme umsetzen.

# 1. Einführung in die Informationssicherheit

## Einführung

Im Vergleich zu früheren Methoden zur Bewältigung von Herausforderungen im Bereich der Informationssicherheit gehen Organisationen heute bewusster mit dem Thema um. Dies ist aufgrund der ständig wachsenden Bedrohungen in diesem Bereich notwendig geworden. Das Risikoniveau, das sich aus der Schwachstellen- und Bedrohungsanalyse ergibt, steigt kontinuierlich und erreicht in einigen Fällen alarmierende Ausmaße. Die Maßnahmen zur Umsetzung der Informationssicherheit müssen mit der Intensivierung der Aktivitäten böswilliger Akteure Schritt halten. Maßnahmen müssen kontinuierlich überprüft, verwaltet und verbessert werden, um den immer komplexeren und raffinierteren Angriffen und Bedrohungsszenarien zu begegnen. Das Ausmaß und die Bedeutung der Herausforderungen im Bereich der Informationssicherheit nehmen ständig zu. Dementsprechend müssen auch die Maßnahmen zu ihrer Bewältigung angepasst und intensiviert werden. Aber wie sieht die Realität aus?

Unternehmen jeder Größenordnung – ob klein, mittel oder groß – haben in letzter Zeit zunehmend finanzielle Verluste aufgrund von Verstößen gegen die Informationssicherheit erlitten. Die Aktivitäten böswilliger Individuen, darunter Hacking, Ransomware, Man-in-the-Middle-Angriffe und andere, zielen darauf ab, Organisationen zu destabilisieren und handlungsunfähig zu machen. Viele Unternehmen und Organisationen haben noch keine ausreichende Resilienz entwickelt, um mit solchen Störungen ihrer Abläufe umzugehen, wenn ihre Sicherheitsmaßnahmen kompromittiert werden. Große Organisationen sind in vielen Fällen unzureichend ausgestattet, um solche Aktivitäten wirksam zu bekämpfen, und handeln eher reaktiv als proaktiv. Infolgedessen werden solche Sicherheitsverletzungen häufig nicht rechtzeitig gemeldet oder bleiben sogar unentdeckt.

IT-Systeme, in denen Informationen erzeugt, gespeichert, transportiert und verarbeitet werden, werden immer ausgefeilter, die Zahl der Beteiligten und die technischen Aspekte immer komplexer. Die zunehmende Komplexität der Thematik erschwert es den Kund:innen, Vertrauen in die Unternehmen zu entwickeln. Es gibt definierte Sicherheitsniveaus, die Organisationen anstreben sollten, um dieses Vertrauen aufzubauen. Standards wie die ISO 27000-Reihe bieten Leitlinien, wie Unternehmen ihre Sicherheitssysteme gestalten können, um Vertrauen bei allen Stakeholdern zu schaffen. Wissenschaftler:innen wie Beckers et al. (2014) weisen darauf hin, dass „die Umsetzung von Sicherheitsstandards aufgrund der begrenzten Unterstützung bei der Systementwicklung und der Dokumentation in den verfügbaren Standards eine Herausforderung darstellt“ (Übers. des Autors).

Um diese Lücke zu schließen, behandelt diese Lektion die wichtigsten Begriffe, Konzepte und Ziele der Informationssicherheit, Sicherheitsstandards und Frameworks und stellt das Informationssicherheitsmanagementsystem (ISMS) vor.

## 1.1 Grundlegende Definitionen, Sicherheitskonzepte und Ziele der Informationssicherheit

Organisationswerte, zu denen auch Informationswerte wie Daten und Informationssysteme gehören, müssen vor sich ständig verändernden Sicherheitsbedrohungen geschützt werden. Es ist unerlässlich, dass Organisationen Sicherheitsaspekte in allen Phasen – Entwicklung, Beschaffung, Installation, Betrieb, Wartung und Außerbetriebnahme – ihrer Organisationswerte berücksichtigen. Dieser Lernzyklus legt die Grundlagen für ein umfassendes Verständnis der Informationssicherheit. Er führt in die grundlegende Terminologie ein und erläutert die zentralen Konzepte und Ziele der Informationssicherheit.

### Geschichte der Informationssicherheit

Nach Whitman und Mattord (2018) beginnt die Geschichte der Informationssicherheit mit dem Konzept der Computersicherheit. Man geht davon aus, dass dieses Konzept während des Zweiten Weltkriegs entstand, als die ersten Großrechner entwickelt wurden. Diese dienten zur Unterstützung von Berechnungen für Kommunikationscodes, die gegen feindliche kryptografische Geräte wie die **Enigma** eingesetzt wurden. Damals wurden, wie aus Berichten hervorgeht, mehrere Sicherheitsstufen eingeführt, um die Geräte und ihre jeweiligen Aufgaben zu schützen. Folglich waren Verfahren und Methoden erforderlich, um die Vertraulichkeit der Daten zu gewährleisten. Der Zugang zu militärischen Einrichtungen wurde teilweise durch Ausweise und physische Schlüssel kontrolliert, und es wurden weitere Maßnahmen ergriffen, um diese sensiblen Geräte und Systeme zu schützen. Der Schutz der nationalen Sicherheit und der Ressourcen war damals bestenfalls rudimentär. Computersicherheit – heute als Informationssicherheit bekannt – war ein unkomplizierter Prozess, der hauptsächlich aus physischer Sicherheit und einfachen Dokumentenklassifizierungssystemen bestand. Die Hauptbedrohungen für die Sicherheit waren der physische Diebstahl von Geräten, Spionage und Sabotage. Im Laufe der Zeit wurden immer komplexere und technologisch anspruchsvollere Maßnahmen zum Schutz von Computersystemen erforderlich, um die nationale Sicherheit zu gewährleisten – einfache und rudimentäre Ansätze reichten nicht mehr aus. Die folgende Tabelle fasst einige der wichtigsten Daten zur Informationssicherheit zusammen.

**Enigma**

Dies war die deutsche Chiffriermaschine, die erst in den 1930er Jahren von polnischen Spezialisten geknackt wurde. Die aus den entschlüsselten Übertragungen gewonnenen Informationen dienten der Vorhersage von Aktionen der deutschen Streitkräfte.

Schlüsseldaten der Informationssicherheit

|  |  |
| --- | --- |
| Datum | Dokument |
| 1968 | Maurice Wilkes spricht über die Sicherheit von *Timesharing-Computern*. |
| 1970 | Willis H. Ware verfasst den Bericht *Security Controls for Computer Systems*: *Report of Defense Science Board Task Force on Computer Security-RAND Report R-609,* der erst 1979 für die Öffentlichkeit freigegeben wurde. Es wurde als bahnbrechende Arbeit bekannt, welche die Notwendigkeit der Computersicherheit aufzeigte. |
| 1973 | Schell, Downey und Popek untersuchen den Bedarf an zusätzlicher Sicherheit in militärischen Systemen in *Preliminary Notes on the Design of Secure Military Computer Systems*. |
| 1975 | Die Federal Information Processing Standards (FIPS) prüft DES (Digital Encryption Standard) im Federal Register. |
| 1978 | Bisbey und Hollingworth veröffentlichen ihre Studie „Protection Analysis: Final Report“, in dem das von der ARPA ins Leben gerufene Projekt „Protection Analysis“ besprochen wurde, um die Schwachstellen der Betriebssystemsicherheit besser zu verstehen und die Möglichkeit automatischer Techniken zur Erkennung von Schwachstellen in bestehender Systemsoftware zu untersuchen. |
| 1979 | Morris und Thompson verfassen „Password Security: A Case History“, veröffentlicht in  *Communications of the Association for Computing Machinery* (ACM). In diesem Artikel wurde die Entwicklung eines Passwortsicherheitssystems für ein Timesharing-System mit Fernzugriff untersucht. |
| 1979 | Dennis Ritchie veröffentlicht „On the Security Of UNIX“ und „Protection of Data File Contents“, in denen sichere Benutzer-IDs, sichere Gruppen-IDs und die mit diesen Systemen verbundenen Probleme behandelt werden. |
| 1982 | Das U.S. Department of Defense Computer Security Evaluation Center veröffentlicht die erste Version der Trusted Computer Security (TCSEC) Dokumente, die als Rainbow Series bekannt wurden. |
| 1984 | Grampp und Morris schreiben „The UNIX System: UNIX Operating System Security“. In diesem Bericht untersuchten die Autoren vier wichtige Voraussetzungen für die Computersicherheit: die physische Kontrolle der Räumlichkeiten und Computereinrichtungen, das Engagement des Managements für die Sicherheitsziele, die Ausbildung der Mitarbeitenden und die Verwaltungsverfahren zur Erhöhung der Sicherheit. |
| 1984 | Reeds und Weinberger veröffentlichen „File Security and the UNIX System Crypt Command“. Ihre Prämisse war: „Es gibt keinen Schutz vor Abhörmaßnahmen oder deren Äquivalent auf dem Computer. Daher kann keine Technik gegen den Systemadministrator oder andere privilegierte Benutzer sicher sein… der naive Benutzer hat keine Chance.“ |
| 1992 | Forscher:innen der Internet Engineering Task Force, die am Naval Research Laboratory arbeiten, entwickeln das Sicherheitsprotokoll Simple Internet Protocol Plus (SIPP) und schaffen damit das, was heute als IPSEC Security bekannt ist. |

Quelle: Andrew Sai (2023), basierend auf Whitman und Mattord (2018).

Wie bereits in diesem Lernzyklus erwähnt wurde, konzentrierte sich die Computersicherheit in der Vergangenheit nur auf den Schutz von Geräten vor Angriffen. Das Internet hat in den letzten Jahren Millionen von Bedrohungen hervorgebracht, die auf die umfangreiche Kommunikation zwischen zahlreichen Computersystemen und Netzwerken zurückzuführen sind, von denen einige ungesichert sind. Seit den 2000er Jahren wächst das Bewusstsein für die Notwendigkeit, die Informationssicherheit zu verbessern. Dieses Bewusstsein geht über die Unternehmensebene hinaus und erkennt an, dass Informationssicherheit für die nationale Sicherheit und Verteidigung von entscheidender Bedeutung ist. Sowohl Regierungen als auch Unternehmen sehen sich zunehmenden Bedrohungen durch **Cyberangriffe** ausgesetzt. Der Schutz computergestützter Steuerungssysteme für öffentliche Versorgungsunternehmen und kritische nationale Infrastrukturen wird immer wichtiger. Darüber hinaus wächst die Besorgnis über Bedrohungen durch Nationalstaaten, die Informationskriege führen. Ein Beispiel hierfür ist der mutmaßliche russische Hackerangriff auf die Ressourcen der Demokratischen Partei der USA während der US-Wahlen 2016 (116. Kongress, 2020).

**Cyberangriff**

Ein böswilliger und vorsätzlicher Versuch einer Person oder Organisation, in das Informationssystem einer anderen Person oder Organisation einzudringen.

### Grundlegende Sicherheitsdefinitionen und Sicherheitskonzepte

Die im Folgenden aufgeführten Definitionen von Informationssicherheit und ausgewählten Konzepten werden in der **ISO**/IEC 27000 bzw. in der ISO/IEC 27000:2014 erläutert oder stammen aus anderen relevanten ISO-Normen. Nach Hintzbergen et al. (2015) ist die ISO/IEC 27000:2014 der erste Teil der gesamten ISO 27000-Normenfamilie und gibt einen Überblick über die Normen und erläutert die in dieser Normenfamilie verwendeten Begriffe. Der Fokus liegt auf Informationstechnologie, Sicherheitstechnik und Informationssicherheitsmanagementsystemen. Ziel dieser Definitionen ist es laut ISO, Verwirrung über Begriffe und Definitionen zu vermeiden und ein einheitliches Verständnis zu schaffen. Hintzbergen et al. (2015) zeigen auf, wie die Autor:innen der ISO 27000-Reihe versuchen, Konsistenz zu gewährleisten und ein gemeinsames Verständnis von Begriffen und Bedingungen zu fördern. Sie weisen darauf hin, dass zum Beispiel „Vermögenswert“ in den Normen als „jedes Objekt, das für eine Organisation von Wert ist“ definiert wird. Dies bedeutet, dass jede Norm, unabhängig vom Thema, die gleiche Definition von „Vermögenswert“ verwendet (Hintzbergen et al. 2015). Im Folgenden werden die für diesen Kurs relevanten Definitionen ausgewählt und erläutert:

**ISO**

Eine internationale Organisation zur Entwicklung von Normen, die sich aus Vertreter:innen der nationalen Normungsorganisationen der Mitgliedsländer zusammensetzt.

**Informationsbezogene Definitionen aus der Norm ISO/IEC 27000**

Die nachstehende Tabelle enthält eine Reihe von Begriffen, die unter den weit gefassten Begriff der informationsbezogenen Definitionen fallen. Diese Begriffe und Konzepte beginnen mit Informationen, die als ein Vermögenswert für eine Organisation zu betrachten sind oder Informationen implizieren.

Informationsbezogene Definitionen aus der Norm ISO/IEC 27000

|  |  |
| --- | --- |
| Begriff | Definition |
| Informationen | Informationen sind Daten, die in einem bestimmten Kontext für den Empfänger eine Bedeutung haben. |
| Informationssicherheit | Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Darüber hinaus können auch andere Eigenschaften wie Authentizität, Nachvollziehbarkeit, Nichtabstreitbarkeit und Zuverlässigkeit eine Rolle spielen. |
| Informationssicherheitsmanagement | Koordinierte Aktivitäten zur Steuerung und Kontrolle einer Organisation im Hinblick auf Risiken. Das Risikomanagement umfasst in der Regel Risikobeurteilung, Risikobehandlung, Risikoakzeptanz und Risikokommunikation. |
| Informationssicherheitsmanagementsystem (ISMS) | Teil des gesamten Managementsystems, das auf einem Geschäftsrisikoansatz basiert, um die Informationssicherheit einzurichten, zu implementieren, zu betreiben, zu überwachen, zu überprüfen, zu erhalten und zu verbessern. Das Managementsystem umfasst Organisationsstrukturen, Politiken, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Verfahren, Prozesse und Ressourcen. |
| Informationssystem | Anwendung, Dienst, IT-Anlage oder jede andere Komponente zur Informationsverarbeitung. |

Quelle: Andrew Sai (2023), basierend auf Hintzbergen et al. (2015).

**Risikobezogene Definitionen aus ISO/IEC 27000 – Vokabular**

In der folgenden Tabelle finden Sie eine Reihe von Begriffen und Konzepten, die mit dem Wort Risiko beginnen oder risikobezogen sind. Diese beziehen sich auf Risiken und wie diese im Kontext des Kurses zu interpretieren sind.

Risikobezogene Definitionen aus ISO/IEC 27000

|  |  |
| --- | --- |
| **Begriff** | **Definition** |
| Restrisiko | Nach der Risikobehandlung verbleibendes Risiko. Das Restrisiko kann ein nicht identifiziertes Risiko enthalten und wird auch als „einbehaltenes Risiko“ bezeichnet. |
| Risiko | Auswirkungen von Unsicherheit auf die Ziele. |
| Risikoakzeptanz | Die Entscheidung, ein Risiko einzugehen. |
| Risikoanalyse | Ein Prozess, um die Art des Risikos zu verstehen und den Grad des Risikos zu bestimmen. Eine Risikoanalyse bildet die Grundlage für die Risikobewertung und Entscheidungen über die Risikobehandlung. Die Risikoanalyse umfasst eine Risikoeinschätzung. |
| Risikobeurteilung | Die Risikobeurteilung ist der Gesamtprozess der Risikoidentifizierung, Risikoanalyse und Risikobewertung. |
| Risikobewertung | Ein Prozess, bei dem die Ergebnisse der Risikoanalyse mit Risikokriterien verglichen werden, um festzustellen, ob das Risiko und/oder sein Ausmaß akzeptabel oder tolerierbar ist. |
| Risikoidentifizierung | Der Prozess des Auffindens, Erkennens und Beschreibens von Risiken. Bei der Risikoidentifizierung geht es um die Identifizierung von Risikoquellen, Ereignissen, ihren Ursachen und ihren möglichen Folgen. Bei der Risikoermittlung können auch historische Daten, theoretische Analysen, fundierte Expertenmeinungen und die Bedürfnisse von Stakeholdern berücksichtigt werden. |
| Risikomanagement | Koordinierte Aktivitäten zur Steuerung und Kontrolle einer Organisation im Hinblick auf Risiken. |
| Risikomanagementprozess | Eine systematische Anwendung von Managementpolitiken, -verfahren und -praktiken auf die Aktivitäten der Kommunikation, der Beratung, der Festlegung des Kontextes und der Identifizierung, Analyse, Bewertung, Behandlung, Überwachung und Überprüfung von Risiken. ISO/IEC 27005:2011, der ISO-Standard für das Risikomanagement im Bereich der Informationssicherheit, verwendet den Begriff „Prozess“, um das Risikomanagement insgesamt zu beschreiben. Die Elemente innerhalb des Risikomanagementprozesses werden als „Aktivitäten“ bezeichnet. |
| Risikobehandlung | Der Prozess der Auswahl und Umsetzung von Maßnahmen zur Risikominderung. |

Quelle: Andrew Sai (2023), basierend auf Hintzbergen et al. (2015).

Weitere Begriffe und Konzepte, wie z. B. Maßnahme, Leitfaden, Vermögenswert, Angriff, Politik, Präventivmaßnahme, Verfahren, Prozess, Drittpartei, Bedrohung und Schwachstelle, die im Kurs ausführlich behandelt werden, finden Sie auf der ISO-Website. Die IEC bietet die *Electropedia* an, die Normen erarbeitet und veröffentlicht und auf der Website der IEC zu finden ist.

### Ziele der Informationssicherheit

Informationssicherheit ist wichtig, um Informationen und andere Organisationsressourcen zu schützen. Diese Informationen können gedruckt, auf einem Computersystem gespeichert oder nur im Kopf der Benutzer:innen vorhanden sein. Der Anwendungsbereich der IT-Sicherheit umfasst daher alle Quellen einschließlich elektronisch gespeicherter Informationen und deren Verarbeitung.

Auch wenn Sicherheitsvorfälle auftreten können oder bereits aufgetreten sind, sollten Sicherheitsmaßnahmen, wenn sie implementiert und wirksam sind, dazu beitragen, das Ausmaß und die Schwere der Sicherheitsbedrohungen, mit denen eine Organisation konfrontiert sein kann, zu minimieren und die Kontinuität der Geschäftstätigkeit und den Erfolg der Organisation zu gewährleisten. Solche Bedrohungen und Schwachstellen können nicht beseitigt werden, aber ihre Auswirkungen können durch geeignete Sicherheitsmaßnahmen minimiert werden, so dass weniger Sicherheitsvorfälle auftreten.

Um ein effektives Informationssicherheitsmanagement zu gewährleisten, sollten Kontrollmaßnahmen auf der Grundlage einer Risikobeurteilung und eines Managementprozesses entwickelt und implementiert werden. Diese Kontrollmaßnahmen sollten in ein Informationssicherheitsmanagementsystem (ISMS) integriert werden. Ein ISMS besteht aus einer Reihe von Richtlinien, Prozessen, Verfahren, Organisationsstrukturen, Software und Hardware, die dazu dienen, die Informationswerte einer Organisation zu schützen. Es ist wichtig, dass das ISMS regelmäßig überprüft wird, um es an Veränderungen anzupassen und Verbesserungen an den Systemen vorzunehmen. Diese Anpassungen sollten auch die Geschäftsziele und andere strategische Ziele der Organisation berücksichtigen. Diese Maßnahmen sollten nahtlos in die bestehenden Geschäftsprozesse integriert und operationalisiert werden.

Die CIA-Triade

Diagramm

Beschreibung automatisch generiert

Quelle: Andrew Sai (2023).

Informationen können wertvoll sein. Der Wert von Informationen beruht auf ihren Eigenschaften, und Änderungen dieser Eigenschaften wirken sich entsprechend auf ihren Wert aus. Die Auswirkungen dieser Veränderungen können je nach Umständen und Nutzer:innen der Informationen unterschiedlich sein.

Um die Ziele zu erreichen, sollten Informationen für die vorgesehenen Nutzer:innen verfügbar, intakt und frei zugänglich sein. Verfügbarkeit, Zugänglichkeit und Integrität von Informationen bedeuten, dass die Nutzer:innen in der Lage sein sollten, rechtzeitig und ohne Beeinträchtigung oder Verzögerung auf die Informationen zuzugreifen. Die Gewährleistung dieser drei Ziele stellt eine Herausforderung für das Informationsmanagement dar. Jeder dieser Aspekte der Triade wird in den folgenden Unterlernzyklen ausführlicher behandelt:

#### Verfügbarkeit

Die ISO/IEC 27001:2013-Normen definieren Verfügbarkeit als „Eigenschaft, auf Verlangen einer autorisierten Stelle zugänglich und nutzbar zu sein“ (Hintzbergen, J. et al., 2015). Bei der Verfügbarkeit von Informationen geht es darum, sicherzustellen, dass die Informationen rechtzeitig zur Verfügung stehen, wenn sie benötigt werden. Es ist allgemein bekannt, dass die beiden anderen Aspekte der Triade (Integrität und Vertraulichkeit) ohne Verfügbarkeit wertlos sind. Die Nutzer:innen sollten in der Lage sein, auf Informationen zuzugreifen, wenn sie die erforderlichen Berechtigungen und Bedingungen erfüllen.

Informationen gelten als verfügbar, wenn autorisierte Benutzer:innen ungehindert auf sie zugreifen können. Ein Beispiel hierfür ist die Online-Bibliothek einer Universität. Benutzer:innen bzw. Besucher:innen solcher Online-Ressourcen müssen sich identifizieren, bevor sie auf Bücher oder Materialien zugreifen können. Autorisierte Benutzer:innen werden in das Online-Bibliothekssystem aufgenommen, und nur sie können auf die Inhalte zugreifen.

Die Verfügbarkeit von Informationen kann durch verschiedene Bedrohungen wie Sabotage, Denial-of-Service-Angriffe oder Ransomware beeinträchtigt werden. Eine Maßnahme zur Abwehr solcher Bedrohungen ist die regelmäßige Sicherung der Informationen. Die Verwendung redundanter Netzwerke, Server und Anwendungen ist eine weitere Maßnahme, um die Verfügbarkeit von Informationen zu gewährleisten.

#### Vertraulichkeit

Die ISO/IEC 27001:2013-Normen definieren Vertraulichkeit als die „Eigenschaft, dass Informationen nicht unbefugten Personen, Einrichtungen oder Prozessen zugänglich gemacht oder offengelegt werden“ (Hintzbergen, J. et al., 2015). Informationen erfüllen die Anforderung der Vertraulichkeit, wenn sie vor Offenlegung oder Weitergabe ohne entsprechende Berechtigung an Personen und Systeme geschützt sind. Im Wesentlichen geht es darum, autorisierten Benutzer:innen Rechte und Privilegien für den Zugriff auf Informationen zu gewähren, die üblicherweise in IT-Systemen gespeichert und verarbeitet werden. Der unbefugte Zugriff auf solche Informationen stellt eine Verletzung der Vertraulichkeit dar. Eine Verletzung der Vertraulichkeit kann auf verschiedene Weise erfolgen. Bei manchen Formen handelt es sich um direkte Angriffe, die darauf abzielen, Zugang zu einem System zu erlangen oder eine Anwendung oder Datenbank zu infiltrieren. Ein Beispiel für direkte Angriffe sind Techniken wie **Man-in-the-Middle**-Angriffe **(MITM)**. Um die Vertraulichkeit von Informationen zu schützen, können diese

**MITM-Angriff**

Dabei handelt es sich um einen Angriff, bei dem sich ein:e Angreifer:in zwischen zwei kommunizierenden Parteien positioniert, um die zwischen ihnen übertragenen Daten abzufangen und/oder zu verändern.

* klassifiziert werden, so dass nur autorisierte Benutzer:innen Zugang zu ihnen haben. Informationen, die mit „Klasse A“ gekennzeichnet sind, könnten z. B. bedeuten, dass sie streng vertraulich und nur für wenige Personen, z. B. das Top-Management, bestimmt sind.
* sicher in Dokumentenspeichern oder mit den richtigen Tools und Ressourcen gespeichert werden.
* durch allgemeine und spezifische Sicherheitsrichtlinien geschützt werden, die den Zugriff und die Nutzung definieren.
* durch Aufklärung und Schulung von Endnutzer:innen und anderen Interessengruppen in Bezug auf die Informationssicherheit geschützt werden.

Verbraucher:innen, die das Internet und Online-Ressourcen nutzen, geben häufig persönliche Informationen über sich preis, um einen bestimmten Komfort oder Mehrwert zu erhalten. Wenn Sie sich kostenlos bei vielen Webportalen und Online-Plattformen anmelden, müssen Sie als Gegenleistung personenbezogene Daten (Personally Identifiable Information, PII) angeben, die von Dritten in der Online-Kette kopiert, verkauft, vervielfältigt oder verbreitet werden.

Vertraulichkeit ist, genau wie andere Eigenschaften von Informationen, nicht isoliert zu betrachten. Sie ist wechselseitig abhängig. Ein Merkmal ist der Datenschutz. Es gibt eine Reihe von Maßnahmen, die ergriffen werden könnten, um die Flut von Datenschutzverletzungen einzudämmen oder besser noch zu verringern. Zu diesen Maßnahmen gehören die Klassifizierung und Beschränkung des Datenzugriffs, die Implementierung von Zugriffskontrollrichtlinien, die Verschlüsselung von Daten und die Aktivierung von Multi-Faktor-Authentifizierungssystemen (z. B. 2FA). Ein weiterer guter Ansatz zur Gewährleistung der Vertraulichkeit ist die Bereitstellung von Schulungen und Wissen, das für alle Beteiligten der Informationskette leicht zugänglich ist.

#### Integrität

Integrität ist das dritte Element der Triade. Die ISO/IEC 27001:2013-Normen definieren Integrität als „Eigenschaft des Schutzes der Genauigkeit und Vollständigkeit von Vermögenswerten“ (Hintzbergen, J. et al., 2015). Die Integrität von Informationen bezieht sich auf die Sicherstellung, dass Daten nicht verändert oder verfälscht wurden. Es geht darum, dass die Informationen vollständig, authentisch, genau und zuverlässig sind.

Die Integrität von Informationen kann auf verschiedene Weise verletzt werden. Ein Beispiel ist, wenn ein:e Angreifer:in ein Intrusion-Detection-System umgeht und Dateikonfigurationen ändert, um einen unbefugten Zugriff zu ermöglichen. Ein weiteres Beispiel ist die Manipulation von Systemprotokollen und Dateien durch eine:n solchen Angreifer:in. Auch unbeabsichtigte Integritätsverletzungen können auftreten, z. B. durch einen Insider wie einen Mitarbeitenden. In solchen Fällen wurden fehlende Sicherheitsrichtlinien, Sicherheitsmaßnahmen, Prozesse und Verfahren als Hauptauslöser identifiziert.

Verschiedene Maßnahmen können ergriffen werden, um die Integrität von Informationen zu schützen. Eine häufig angewandte Methode ist das Hashing oder die Verwendung von Hash-Algorithmen, um die Integrität von Daten zu überprüfen. Datenverschlüsselung, digitale Zertifikate und Signaturen sowie die Verwendung vertrauenswürdiger Zertifizierungsstellen (CAs) sind weitere Maßnahmen, die zur Sicherstellung der Integrität eingesetzt werden können. Nichtabstreitbarkeit, d. h. die Unmöglichkeit, etwas zu leugnen oder zu widerlegen, wird ebenfalls verwendet, um die Authentizität und Integrität von Informationen zu gewährleisten.

Mechanismen zur Wahrung der Informationsintegrität werden häufig in präventive und detektive Mechanismen unterteilt. Die häufigste Integritätsverletzung ist die unbeabsichtigte Offenlegung (Alsmadi I., et al. 2018). Benutzer:innen, insbesondere Mitarbeitende von Organisationen, können Informationen verlieren, verlegen oder versehentlich preisgeben, ohne dass dies durch Hacker oder einen elektronischen Angriff verursacht wurde. So posten beispielsweise manche unachtsame Mitarbeitende von Organisationen in sozialen Netzwerken Bilder ihrer Arbeitsplatzbildschirme, auf denen sensible Informationen offen zu sehen sind. Das ist eine unbeabsichtigte Offenlegung. Andere nehmen Kopien ihrer Organisationsdaten mit, die E-Mail-Adressen, Kreditkarteninformationen, Ausweisnummern oder wichtige Unternehmensdateien enthalten können, und verlieren diese durch Diebstahl, Kriminelle oder andere böswillige Benutzer:innen.

### Fragen zur Selbstkontrolle

1. Welches der folgenden Merkmale wird verwendet, um sicherzustellen, dass die Korrektheit der Informationen in der Organisation effektiv abgedeckt ist?

* *Integrität*
* Vertraulichkeit
* Verfügbarkeit
* Authentizität

1. Ein:e Benutzer:in meldet sich bei einem Computersystem an und wird aufgefordert, eine Sicherheitsfrage zu beantworten, z. B. „Wie lautet der Mädchenname Ihrer Mutter?“ Welchen der folgenden Punkte gewährleistet das Computersystem?

* Rechenschaftspflicht
* *Authentifizierung*
* Autorisierung
* Anwendbarkeit

1. Bitte vervollständigen Sie den folgenden Satz.

Die *Enigma* war eine *deutsche* Chiffriermaschine, die erstmals in den 1930er Jahren von *polnischen* Spezialisten geknackt wurde.

## 1.2 Normen und regulatorische Rahmenbedingungen

**Normen** werden oft als starr und weltweit allgemein akzeptiert angesehen. Ein Framework ist bestenfalls ein Rahmen, der als Vorgehensweise genutzt werden kann. („Unterschied zwischen Norm und Framework“, o. J.) Normen wurden entwickelt, um die Art und Weise zu harmonisieren, in der Produkte und Dienstleistungen an Verbraucher:innen geliefert werden, sei es von einer staatlichen Stelle oder Behörde an eine:n Bürger:in eines Landes oder ein neues Medikament, z. B. für Krebspatient:innen, das von einem Pharmaunternehmen entwickelt wird.

**Normen**

Normen sind Dokumente, die von einem anerkannten Gremium, wie der International Standards Organization (ISO) veröffentlicht wurden, um ein gemeinsames Verständnis der Spezifikationen und Prozesse zu vermitteln, die für die Lieferung von zuverlässigen Produkten und Dienstleistungen erforderlich sind.

Normen, die in der Regel nicht verpflichtend sind, definieren spezifische Protokolle und Anforderungen für Produkte wie z. B. ein Informationssicherheitsmanagementsystem, so dass die Integration in eine Organisation weltweit gleich ist. Daher wird die Implementierung eines ISMS weltweit einheitlich sein. Es handelt sich größtenteils um Empfehlungen zu Best Practices. Im Falle des ISMS dienen die einschlägigen Normen dem/r Sicherheitsbeauftragten als grundlegendes Referenzmodell für die Bereitstellung von Sicherheitskapazitäten und die Festlegung von Methoden zur Durchführung von Sicherheitsmaßnahmen, die leicht in der gesamten Organisation angewendet werden können. Normen helfen Unternehmen sicherzustellen, dass Pläne, Richtlinien, Verfahren, Kontroll- und andere Maßnahmen mit den Erwartungen der Branche und den globalen Erwartungen übereinstimmen und angemessen sind. Dies schafft zusätzliche Sicherheit, die den rechtlichen und wirtschaftlichen Anforderungen entspricht.

Im Gegensatz zu Normen sind **regulatorische Rahmenbedingungen** (auch Rahmenwerke oder Frameworks) rechtliche Mechanismen, die sowohl auf nationaler als auch auf internationaler Ebene anwendbar sind und verbindlichen oder verpflichtenden Charakter haben. Eine Organisation, die sich weigert, gesetzliche oder behördliche Anforderungen zu erfüllen, muss bei Nichteinhaltung mit Konsequenzen rechnen. Das bedeutet, dass das pharmazeutische Unternehmen, welches die Krebsmedikamente herstellt, bei Nichteinhaltung der gesetzlichen Vorschriften Gefahr läuft, seine existenzsichernde Lizenz oder Zertifizierung zu verlieren, oder in bestimmten Fällen mit Geldstrafen und anderen Sanktionen belegt zu werden. Normen sind nicht einklagbar, sondern Empfehlungen für bewährte Verfahren. Wenn eine Norm z. B. verlangt, dass einige Mitglieder des Vorstandes eines Unternehmens Kenntnisse oder frühere Arbeitserfahrungen in der pharmazeutischen Industrie haben sollten, so ist dies keine Verpflichtung, sondern eine Empfehlung.

**Regulatorische Rahmenbedingungen**

Ein verbindliches Regelwerk (Instrumente, Gesetze, Verordnungen, Vorschriften, Verfahren, Abschlüsse).

Es gibt unzählige regulatorische Frameworks für die Informationstechnologie. Einige dieser Frameworks sind der Federal Information Security Management Act (FISMA), die ISO/IEC 27001 und 27002, die Control Objectives for Information and Related Technologies (COBIT) und viele andere. Es ist erwähnenswert, dass die meisten dieser Frameworks regelmäßig überprüft und aktualisiert werden. So wurde beispielsweise das COBIT-Framework, das Komponenten und Designfaktoren für den Aufbau und die Aufrechterhaltung eines Governance-Systems, einschließlich der Informationssicherheit, in einer Organisation definiert, kürzlich zu COBIT 2019 aktualisiert und 2018 veröffentlicht, während ISO/IEC 27001:2022 – *Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen* – aktualisiert und 2022 veröffentlicht wurde. Darüber hinaus gibt es weitere, die von NIST und ENISA herausgegeben werden. Einige decken branchenspezifische Bereiche ab, während andere sich auf kritische Infrastrukturen und deren Schutz konzentrieren. Andere wiederum dienen dem Datenschutz und dem Schutz der Privatsphäre.

Laut Landoll (2016), in *Information Security Policies, Procedures and Standards*, Seite 20-21, sind „Informationssicherheitsnormen eine Verfeinerung der Sicherheitsanforderungen in den Informationssicherheitsrichtlinien, die ausgewählte Methoden, Techniken und Geräte betreffen. Diese Normen sind obligatorisch, da sie die erforderlichen Verfeinerungen der Informationssicherheitsrichtlinien festlegen. Normen werden in der Regel entweder von der Geschäftsleitung oder von deren Beauftragten wie dem/r Informationssicherheitsbeauftragten oder dem/r Informationssicherheitsmanager:in herausgegeben und genehmigt…. Informationssicherheitsnormen werden entwickelt, um die Erklärungen auf der Ebene der Informationssicherheitspolitik zu erläutern oder zu präzisieren. Aus diesem Grund sollten Informationssicherheitsnormen einen direkten und klaren Bezug zur Erklärung der Informationssicherheit haben, die sie verfeinern…“ (Übers. des Autors). Ein Beispiel für eine Standarderklärung könnte lauten: „Die Organisation sollte sicherstellen, dass alle Informationssysteme, die eine passwortbasierte Authentifizierung verwenden, die folgenden Mindestparametereinstellungen durchsetzen: (a) Passwortkomplexität – 8 Zeichen mit sowohl numerischen als auch alphabetischen Zeichen, (b) Passwortlebensdauer – maximal 60 Tage, mindestens 1 Tag, (c) Passwortwiederverwendung – 6 Generationen“ (Landoll, 2016, S. 20-21, Übers. des Autors).

Für den Aufbau eines ISMS gibt es zwei Hauptnormen, ISO/IEC 27001 und ISO/IEC 27002, die die Anforderungen und erforderlichen Verfahren für den Aufbau eines ISMS festlegen, was eine wichtige Audit- und Compliance-Tätigkeit darstellt. Die Basisnorm ISO/IEC 27000 enthält eine Übersicht und das Vokabular, das im Wesentlichen das zu implementierende ISMS-Programm definiert. Die ISO/IEC 27000-Reihe wird in dieser Lektion ausführlich behandelt.

Neben den primären Normen (hauptsächlich die ISO/IEC 27000-Normenfamilie) gibt es weitere verwandte Normen und Frameworks, die zusammenwirken, um Compliance- und Audit-Anforderungen zu erfüllen und in vielen Fällen eine Zertifizierung in verschiedenen Bereichen zu erreichen. Solche Sicherheits-Frameworks sind häufig auf bestimmte Branchen und Sektoren ausgerichtet. Es gibt eine Vielzahl solcher Normen, von denen einige in diesem Kurs erwähnt werden. Eine kurze Liste der gebräuchlichsten wird im Folgenden vorgestellt und in den folgenden Unterlektionen diskutiert. Es ist zu beachten, dass die ISO/IEC 27001 zwar eine Zertifizierung zulässt, diese aber im Allgemeinen nicht obligatorisch ist, mit einigen Ausnahmen in bestimmten Branchen.

Die folgende Abbildung zeigt einige der gängigsten Sicherheitsnormen und -Frameworks.

Gängige Sicherheitsnormen und -Frameworks

Form

Beschreibung automatisch generiert

Quelle: Andrew Sai (2023).

Im Folgenden werden diese gängigen Sicherheitsnormen und regulatorischen Rahmenbedingungen, die einem Unternehmen für den Schutz von Sicherheitsressourcen zur Verfügung stehen, in keiner bestimmten Reihenfolge erläutert.

### Common Criteria for Information Technology Security Evaluation

ISO/IEC 15408, auch bekannt als Common Criteria (CC), ist ein internationaler Standard für die Sicherheit von IT-Produkten, einschließlich Betriebssystemen und Firewalls. Im Jahr 2017 wurde die aktuelle Version 3.1 Revision 5 veröffentlicht. CC bietet Spezifikationen und Leitfäden für die Bewertung von Informationssicherheitsprodukten und -systemen. Dieser Standard wurde im Rahmen eines Abkommens mit der Bezeichnung **CCRA** entwickelt und gepflegt. CC dient als Leitfaden für die Entwicklung, Bewertung und Beschaffung von IT-Produkten mit Sicherheitsfunktionen und bildet im Wesentlichen die Grundlage für die Bewertung der Sicherheitseigenschaften von IT-Produkten. Beispiele für nach ISO/IEC 15408 zertifizierte Produkte sind Microsoft Windows 10, Apple iOS, Samsung Knox, Oracle-Datenbank, IBM WebSphere Application Server und viele andere.

**CCRA**

Das Abkommen über die Anerkennung von Common-Criteria-Zertifikaten im Bereich der IT-Sicherheit ist ein Abkommen der teilnehmenden Nationen.

CC bietet einen Rahmen für die Definition von Sicherheitsanforderungen, die Bewertung von Sicherheitsmerkmalen und die Zertifizierung von IT-Produkten und -Systemen, die bestimmte Standards erfüllen. Nachfolgend finden Sie sechs der wichtigsten CC-Konzepte und wie sie zur Sicherung von IT-Produkten und -Systemen eingesetzt werden:

1. **Protection Profile (PP, Schutzprofil)**: Dies ist ein Dokument, das die erforderlichen Sicherheitsfunktionen und Zuverlässigkeitsanforderungen für ein bestimmtes Produkt oder System festlegt. Durch die Definition einer Reihe von grundlegenden Sicherheitsanforderungen können IT-Produktentwickler:innen sicherstellen, dass ihre Produkte ein bestimmtes Sicherheitsniveau einhalten. Schutzprofile können branchenübergreifend angewendet werden und ermöglichen so eine Standardisierung und Konsistenz bei der Entwicklung sicherer IT-Produkte.
2. **Security Target** **(ST, Sicherheitsvorgaben)**: Dies ist ein Dokument, das eine detaillierte Beschreibung der Sicherheitseigenschaften eines bestimmten Produkts oder Systems enthält, einschließlich seiner Sicherheitsziele, Bedrohungen und funktionalen Anforderungen. Ein ST wird verwendet, um nachzuweisen, dass ein Produkt oder System bestimmte Sicherheitsanforderungen erfüllt, die im zugehörigen Schutzprofil definiert sind. Durch die Prüfung eines ST können die Evaluator:innen feststellen, ob das Produkt oder System angemessene Sicherheitsmaßnahmen zur Abwehr potenzieller Sicherheitsbedrohungen bietet.

**Evaluation Assurance Level** Das EAL eines IT-Produkts oder -Systems ist eine numerische Note, die nach Abschluss einer CC-Evaluation vergeben wird.

1. **Evaluation Assurance Level (EAL)**: Dies ist ein numerischer Wert (von EAL1 bis EAL7), der die Gründlichkeit und Tiefe der Sicherheitsbewertung eines IT-Produkts angibt. Höhere EAL-Stufen bedeuten eine größere Sicherheit, dass das Produkt gründlich getestet wurde und resistent gegen Angriffe ist. Durch den Evaluierungsprozess erhalten IT-Produkte und -Systeme ein EAL, das auf dem Grad der Einhaltung der CC-Standards basiert und es Kund:innen ermöglicht, fundierte Entscheidungen über die Sicherheit ihrer IT-Produkte zu treffen.
2. **Target of Evaluation (TOE, Evaluationsgegenstand)**: Dies bezieht sich auf das IT-Produkt oder -System, das hinsichtlich seiner Sicherheitseigenschaften evaluiert wird, z. B. Software, Hardware oder eine Kombination aus beidem. Das TOE steht im Mittelpunkt des Evaluierungsprozesses und muss ausreichende Informationen über die Eigenschaften und Funktionen des Produkts liefern, um eine gründliche Sicherheitsbewertung zu ermöglichen.
3. **Annahmen und Bedrohungen**: Dies sind die Bedingungen, die außerhalb des TOE erfüllt sein müssen, damit ein Produkt oder System seine Sicherheitsziele erreichen kann. Bedrohungen sind potenzielle Ereignisse oder Aktionen, welche die Sicherheit eines IT-Produkts gefährden könnten. Die Identifizierung und Bewältigung dieser Annahmen und Bedrohungen ist entscheidend für die Entwicklung eines umfassenden Sicherheits-Frameworks für IT-Produkte und -Systeme.
4. **Security Functionality (SF, Sicherheitsfunktionalität) und Security Functional Requirements (SFR, Funktionale Sicherheitsanforderungen)**: SF bezieht sich auf die Merkmale und Fähigkeiten eines IT-Produkts, die zu seinen Sicherheitszielen beitragen. SFRs sind spezifische Sicherheitsfähigkeiten, über die ein Produkt verfügen muss, um die im Schutzprofil definierten Sicherheitsziele zu erfüllen. Die Entwicklung gut definierter SF und SFR gewährleistet, dass IT-Produkte und -Systeme die gewünschten Sicherheitsziele erreichen.

Die teilnehmenden Länder verfügen über Prüforganisationen, die eine Reihe von Sicherheitsanforderungen und Bewertungskriterien anwenden, um die Sicherheit von IT-Produkten und -Systemen zu beurteilen. Der Zertifizierungsprozess umfasst eine strenge Bewertung durch eine akkreditierte Bewertungseinrichtung, das so genannte EAL-Labor. In Deutschland dient beispielsweise das Bundesamt für Sicherheit in der Informationstechnik (BSI) als nationale Zulassungsbehörde. Die Agence nationale de la sécurité des systèmes d'information (ANSSI) ist die Genehmigungsbehörde in Frankreich. Außerhalb der EU sind dies in den Vereinigten Staaten die National Information Assurance Partnership (NIAP), in Kanada das Communication Security Establishment (CSE) und in Japan die Information Technology Promotion Agency (IPA).

Die Normen ISO/IEC 15408 oder CC bieten einen systematischen Ansatz zur Bewertung und Gewährleistung der Sicherheit von IT-Produkten und -Systemen. Die Konzepte und Methoden innerhalb des Frameworks, wie PP, Sicherheitsvorgaben und EAL, tragen zu einem standardisierten und konsistenten Prozess für die Bewertung und Zertifizierung der Sicherheit von IT-Produkten in verschiedenen Branchen bei. Auf diese Weise können Organisationen fundierte Entscheidungen bei der Auswahl von Produkten mit geeigneten Sicherheitsmaßnahmen zum Schutz vor potenziellen Bedrohungen treffen.

### NIST-Sicherheitsstandards und Leitfäden

Das erstmals 2014 veröffentlichte NIST Cybersecurity Framework (CSF) ist ein sehr beliebtes Framework, das als Leitfaden für das Management von **Cybersicherheits**risiken dienen soll. Das NIST CSF bietet eine übergeordnete Taxonomie von Cybersicherheitsergebnissen und eine Methodik zur Bewertung und Verwaltung der Ergebnisse. Es ist eines von über 1300 Standardreferenzmaterialien (SRM), die das amerikanische National Institute of Standards and Technology (NIST) der Industrie, der Wissenschaft, Regierungen und anderen Nutzern des NIST Cyber Security Framework zur Verfügung stellt. Das CSF enthält auch Leitlinien zum Schutz der Privatsphäre und der Bürgerrechte im Bereich der Cybersicherheit. Das CSF ist in drei Hauptteile unterteilt:

**Cybersicherheit**

Dies bezieht sich auf den Schutz von Daten, die in elektronischer Form vorliegen, vor Angriffen oder Kompromittierung. Informationssicherheit bezieht sich auf den Schutz von Informationen und Informationswerten.

1. **Framework-Kern**: Hier finden sich Aktivitäten, Ergebnisse und Hinweise zu Eigenschaften und Methoden der Cybersicherheit.
2. **Framework-Profil**: Dies ist die Liste der Ergebnisse, die eine Organisation aus einer Reihe von Kategorien und Unterkategorien auswählt, nachdem sie die Risiken und ihre geschäftlichen Anforderungen bewertet hat.
3. **Framework-Implementierungsebenen**: Diese werden von Organisationen verwendet, um die Sichtweise einer Organisation in Bezug auf Cybersicherheitsrisiken und ihre Herangehensweise an diese Risiken zu verdeutlichen.

Neben dem CSF, das eine gemeinsame Sprache und Leitfäden für das Sicherheitsmanagement in einer Organisation bietet, gibt es die NIST Special Publication (SP) 1800-Serie. Diese bietet ebenfalls Anleitungen zur Informationssicherheit, einschließlich Risikomanagement, Reaktion auf Vorfälle und Supply-Chain-Sicherheit. Zu den spezifischen Standards innerhalb dieser NIST SP 1800 gehören die NIST SP 800-53 und NIST SP 800-171. Sie dienen als Leitfaden für die Implementierung und Anwendung standardbasierter Sicherheitstechnologien.

**EU-Verordnung**

Dabei handelt es sich um eine Art Rechtsakt, der in allen EU-Ländern direkt anwendbar und verbindlich ist, ohne dass nationale Durchführungsmaßnahmen erforderlich sind.

### Agentur der Europäischen Union für Cybersicherheit (ENISA)

Die gemeinhin als ENISA-Standards bezeichneten Normen sind EU-Normen, Frameworks, Vorschriften und Leitfäden, die Ratschläge und Lösungen zur Verbesserung der Cybersicherheitskapazitäten in der EU bieten. Die Agentur wurde 2004 durch die **EU-Verordnung** Nr. 460/2004 eingerichtet und hat die Aufgabe, ein gemeinsames Niveau der Cybersicherheit in der gesamten europäischen Region zu erreichen. Die Agentur trägt zur Cyberpolitik der EU bei, indem sie das Vertrauen in IKT-Produkte, -Dienstleistungen und -Verfahren durch Zertifizierungssysteme für Cybersicherheit aufrechterhält und die EU-Mitgliedstaaten dabei unterstützt, sich angemessen auf künftige Herausforderungen im Bereich der Cybersicherheit vorzubereiten.

ENISA bietet unter anderem zahlreiche Tools zur Messung des Reifegrads, zur Selbstbewertung und zum Risikomanagement. Einige der gängigsten ENISA-Tools sind die folgenden:

* das Tool zur Selbsteinschätzung des Reifegrads von Computer Security Incident Response Teams (CSIRT)
* das Tool National Cybersecurity Assessment Framework (NCAF)
* SecureSME, das sich an kleine und mittlere Unternehmen richtet, um sie vor Cyberangriffen zu schützen
* Smartphone-Guidelines-Tools für Entwickler:innen von Smartphone-Anwendungen
* bewährte Praktiken für die Sicherheit von Gesundheitsdienstleistungen
* das Online-Tool für die Sicherheit der Verarbeitung personenbezogener Daten
* das Tool Payment Services Directive 2 (PSD2), eine interaktive Karte zur Gewährleistung der Sicherheit von Zahlungen und anderen Finanztransaktionen.

Sicherheitsvorschriften und -richtlinien wurden bewusst zum Schutz kritischer Infrastrukturen entwickelt, und die ENISA, die wichtigste EU-Agentur, die für die Cybersicherheit der Mitgliedstaaten zuständig ist, nimmt die gleichen Aufgaben wahr. Beispiele für solche Richtlinien sind:

#### Schutz von Netzwerk- und Informationssystemen (NIS)

Die **EU-Richtlinie** 2016/1148 zielt darauf ab, das Niveau der Cybersicherheit und die Widerstandsfähigkeit kritischer Systeme in der gesamten EU zu erhöhen. Sie wurde 2016 eingeführt und soll sicherstellen, dass die EU-Mitgliedstaaten über einen nationalen Rahmen (einschließlich einer nationalen Sicherheitsstrategie, einer zuständigen NIS-Behörde und eines CSIRT) verfügen, der es ihnen ermöglicht, Cybersicherheitsvorfälle zu bewältigen und gleichzeitig die Richtlinien umzusetzen. Es wird erwartet, dass diese Richtlinien von jedem EU-Mitgliedstaat in nationales Recht umgesetzt werden. In Deutschland spielt das BSI als Aufsichts- und Durchsetzungsorgan eine zentrale Rolle bei der Umsetzung der NIS-Richtlinie. Die Richtlinie stellt auch sicher, dass die Mitgliedstaaten an einer Arbeitsgruppe für strategische Sicherheitskooperation und Netzwerke teilnehmen und Informationen austauschen.

#### NIS2

**EU-Richtlinie**

Dies ist eine Art Rechtsakt der EU, der ein Ziel festlegt, das von allen EU-Ländern erreicht werden muss, wobei es den einzelnen Ländern überlassen bleibt, wie sie es in nationales Recht umsetzen.

Die NIS2-Richtlinie (**EU-Richtlinie** 2022/2555) wurde im Jahr 2022 eingeführt und trat 2023 in Kraft. Sie modernisiert den bestehenden NIS-Rechtsrahmen, um den aktuellen Entwicklungen im Cyberspace Rechnung zu tragen, und weitet seinen Anwendungsbereich auf zusätzliche Sektoren und Einrichtungen aus, während gleichzeitig die Reaktion auf Zwischenfälle und die Widerstandsfähigkeit kritischer Infrastrukturen in der EU verbessert werden. Das Hauptziel von NIS2 ist die Verbesserung der Cybersicherheit in der gesamten EU durch

* die Einrichtung einer Cyber-Krisenmanagementstruktur (CyCLONe).
* die verbesserte Harmonisierung der Sicherheitsanforderungen und Meldepflichten in den Mitgliedstaaten.
* den Verweis darauf, wie wichtig es ist, Bereiche wie Supply Chain, Schwachstellenmanagement, Internet und Cyber-Hygiene in die nationalen Sicherheitsstrategien der Mitgliedstaaten einzubeziehen.
* die Förderung innovativer Ansätze, wie z. B. Peer Reviews, um die Zusammenarbeit und den Informationsaustausch zwischen den EU-Mitgliedstaaten zu fördern.
* die Ausweitung des Erfassungsbereichs auf weitere Unternehmen und Sektoren, die ursprünglich nicht von der ursprünglichen NIS-Richtlinie erfasst wurden.

Mit der Einführung von NIS2 werden auch der ENISA, der EU-Agentur für Cybersicherheit, verschiedene Aufgaben zugewiesen. Zu ihren Hauptaufgaben gehören die Entwicklung und Pflege eines EU-Registers für Schwachstellen, die Wahrnehmung der Sekretariatsaufgaben für CyCLONe, die Veröffentlichung von Jahresberichten über den Stand der Cybersicherheit in der EU, die Unterstützung von Peer Reviews zwischen den Mitgliedstaaten und die Führung eines Registers von Stellen, die grenzüberschreitende Dienste wie die Registrierung von Domänennamen, Cloud Computing und Rechenzentrumsdienste anbieten. Von den Mitgliedstaaten wird erwartet, dass sie diese Änderungen in ihre nationale Gesetzgebung übernehmen.

#### EU-Richtlinie zum Schutz kritischer Infrastrukturen (RCE)

Die RCE-Richtlinie ist Teil eines Gesetzgebungspakets, das den Schutz der Cybersicherheit und der kritischen Infrastrukturen in der EU sowie die Reaktionsfähigkeit der zuständigen Stellen und Behörden verbessern soll. Die 2020 von der Europäischen Kommission vorgeschlagene RCE-Richtlinie zielt darauf ab, einen gemeinsamen Zertifizierungsrahmen für Cybersicherheit zu schaffen, die Cybersicherheitsforschung und -innovation zu fördern und die Cybersicherheitsbranche in der EU zu stärken.

Zu den weiteren von der ENISA entwickelten und verwalteten Frameworks, Standards und Leitfäden gehören die folgenden:

* Der EU-Rahmen für die Cybersicherheitszertifizierung
* Cybersecurity Culture in Organizations
* Baseline Security Recommendations for Internet of Things (**IoT**)
* Cloud-Sicherheitsleitfaden für KMU

### Branchenspezifische Standards

Verschiedene Standards, Frameworks, Vorschriften und Leitfäden sorgen für Qualität, Sicherheit und Konsistenz in verschiedenen Sektoren und Branchen. Organisationen in bestimmten Branchen und Sektoren müssen diese genauen Anforderungen erfüllen. Beim Aufbau eines ISMS sollten neben den primären ISO/IEC-Normen für den Aufbau und das Management des ISMS auch relevante Normen und Frameworks berücksichtigt werden, um eine kollektive Compliance zu gewährleisten. Es gibt eine Vielzahl von Standards und Frameworks. Die folgenden sind die gängigsten:

* **ISO/IEC 13485:2016 (Qualitätsmanagementsystem für Medizinprodukte):** Dies ist eine umfassende Liste von Anforderungen, die erfüllt werden müssen, um die Qualität der Entwicklung und Herstellung von Medizinprodukten zu gewährleisten.
* **AS9100 (Qualitätsmanagementsystem für die Luft- und Raumfahrt):** Dies ist ein spezieller Standard für die Luft- und Raumfahrtindustrie. Er bietet einen Rahmen für das Qualitätsmanagement in diesem Sektor, der sich mit Sicherheit, Zuverlässigkeit, der Einhaltung von Vorschriften und Risikomanagement befasst.
* **Gefahrenanalyse und kritische Kontrollpunkte (HACCP):** Dieses System wird in der Lebensmittelindustrie eingesetzt, um die Sicherheit von Lebensmitteln zu gewährleisten. Mögliche Gefahren werden identifiziert, Kontrollmaßnahmen eingeführt und die Wirksamkeit der Systeme überwacht.
* **Gute Herstellungspraxis (GMP):** Dies ist ein Standard, der von der pharmazeutischen und medizintechnischen Industrie verwendet wird, um sicherzustellen, dass die Produkte konsistent hergestellt werden und den Qualitätsstandards entsprechen. Er deckt alle Aspekte der Herstellung ab, von den Rohstoffen bis zu den fertigen Produkten.
* **FSSC 22000 (Zertifizierung von Lebensmittelsicherheitssystemen):** Dies ist ein Standard für die Zertifizierung von Managementsystemen für die Lebensmittelsicherheit, der die gesamte Lieferkette abdeckt. Er kann mit dem HACCP-Konzept und anderen lebensmittelbezogenen Sicherheitsanforderungen wie ISO/IEC 22000 und ISO/TS 22002-1 integriert werden.
* **ISO/SAE 21434 (Cybersicherheit für Straßenfahrzeuge):** Dabei handelt es sich um eine neue Norm, die die Sicherheitsanforderungen in der Automobilindustrie festlegt. Sie wurde von der ISO und der Society for Automotive Engineers (SAE) entwickelt und bietet der Industrie einen einheitlichen Rahmen für den Umgang mit Sicherheitsrisiken. Die Standards konzentrieren sich auf die Cybersicherheit von Straßenfahrzeugen.
* **EN 50128 – Bahnanwendungen (Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme):** Dies sind Standards für die Entwicklung von Software für Eisenbahnsteuerungs- und -sicherungssysteme. Die Anwendung dieser Standards gewährleistet die Sicherheit und Zuverlässigkeit des Eisenbahnbetriebs durch die Entwicklung zuverlässiger Software. Die Standards tragen zur Gewährleistung der Sicherheit und des Betriebs kritischer Infrastrukturen in der EU bei.
* **IEC 62443:** Dies ist eine von der International Electrotechnical Commission (IEC) herausgegebene Norm, die einen Rahmen für die Sicherung von industriellen Automatisierungs- und Leitsystemen bietet, wie sie typischerweise zum Schutz kritischer Infrastrukturen in den Bereichen Energie und Transport eingesetzt werden.
* **ISO/IEC 27017:** Dies ist ein Sicherheits-Framework für die Nutzung von Cloud-Diensten. ISO/IEC 27017 ist Teil der Normenfamilie ISO/IEC 27000, die Anbieter von Cloud-Diensten bei der Einhaltung von Vorschriften zum Schutz ihrer Kund:innen und Nutzer:innen unterstützen soll.
* **SOC (Service Organisation Controls) für Cybersicherheit:** Dabei handelt es sich um ein Cybersicherheits-Framework, das vom American Institute of Certified Public Accountants (AICPA) entwickelt wurde, um einen standardisierten Ansatz für die Bewertung und Berichterstattung des Risikomanagementprogramms einer Organisation zu bieten.

### Andere Standards und Frameworks

Die folgenden Standards und Framework sind nicht unbedingt branchenspezifisch. Sie haben einen gewissen Bezug zur IT-Sicherheit, wenn auch nicht immer explizit. Sie werden branchen- und sektorübergreifend angewendet, wo dies sinnvoll ist.

* **OHSAS 18001/ISO/IEC 45001 (Managementsystem für Gesundheit und Sicherheit am Arbeitsplatz):** Diese Norm unterstützt Organisationen bei der Entwicklung eines systematischen Ansatzes für das Management von Gesundheits- und Sicherheitsrisiken am Arbeitsplatz. Sie soll dazu beitragen, arbeitsbedingte Verletzungen zu vermeiden und eine übergreifende Sicherheitskultur zu fördern.
* **ISO/IEC 9001 (Qualitätsmanagementsystem):** Dies wird von einer Vielzahl von Branchen genutzt, um Qualitätssysteme aufzubauen und aufrechtzuerhalten. Im Mittelpunkt stehen Kundenzufriedenheit, kontinuierliche Verbesserung und die Einhaltung gesetzlicher und behördlicher Vorschriften.
* **ISO/IEC 14001 (Umweltmanagementsystem):** Diese Norm bietet Organisationen einen Rahmen für ein verantwortungsvolles und nachhaltiges Management ihrer Umweltverpflichtungen. Sie zeigt auf, wie Organisationen ihre Umweltauswirkungen minimieren, die gesetzlichen Anforderungen erfüllen und ihre Leistung verbessern können.
* **ISO/IEC 22301 (Business Continuity Management System):** Organisationen, die ein Business Continuity Management System (BCMS) nach ISO/IEC 22301 implementieren, können ein formelles Evaluationsverfahren durchlaufen, um eine Akkreditierung nach dieser Norm zu erhalten. Es ist ein Nachweis für die Einhaltung der bewährten Verfahren im Bereich des BCMS durch die Organisation.
* **Kontrollziele für Informations- und verwandte Technologien (COBIT):** Hierbei handelt es sich um ein Framework für Best Practices im Bereich IT-Governance und -Management. Es wird von der Information Systems Audit and Control Association (ISACA) entwickelt und verwaltet. Das COBIT-Framework für Informationssicherheit schafft ein unternehmensweites IT-Governance-System, das verschiedene Sicherheitsmaßnahmen durch eine Reihe strenger Politiken und Regeln implementiert, die die Unternehmenssicherheit insgesamt stärken.
* **Information Technology Infrastructure Library (ITIL):** Hierbei handelt es sich um ein weltweit eingesetztes Framework für das Service Management, das einen speziellen Teil, das Information Security Management (ISM), enthält, um die IT- und die Geschäftssicherheit in einem Unternehmen aufeinander abzustimmen und sicherzustellen, dass diese durchgängig gemanagt werden.
* **Framework des Committee of Sponsoring Organizations (COSO):** Dies ist ein weit verbreitetes Framework für die interne Kontrolle der Finanzberichterstattung. COSO hat kürzlich ein Framework speziell für das Risikomanagement im Bereich der Cybersicherheit entwickelt.

Zusammenfassend lässt sich sagen, dass die in diesem Unterlernzyklus erwähnten Standards und Frameworks mehrere Gemeinsamkeiten aufweisen, u. a.:

* **Sie sind nicht branchenspezifisch:** Sie können je nach Relevanz und Anwendbarkeit in verschiedenen Branchen und Sektoren eingesetzt werden.
* **Sie haben eine Beziehung zur IT-Sicherheit:** Sie befassen sich zwar nicht explizit mit IT-Sicherheit, haben aber einen gewissen Bezug dazu. COBIT und ITIL haben zum Beispiel spezifische Komponenten für das Informationssicherheitsmanagement.
* **Sie fördern einen systematischen Ansatz:** Sie bieten jeweils eine strukturierte Methodik für das Management verschiedener Aspekte einer Organisation, wie Gesundheit und Sicherheit am Arbeitsplatz, Qualität, Umweltauswirkungen, Geschäftskontinuität, IT-Governance und Finanzberichterstattung.
* **Sie setzen auf kontinuierliche Verbesserung**: Sie konzentrieren sich auf die kontinuierliche Verbesserung der Prozesse, Systeme und der Gesamtleistung einer Organisation.
* **Sie fördern die Einhaltung der gesetzlichen und behördlichen Vorschriften:** Die Einhaltung dieser Standards und Frameworks hilft Organisationen, die einschlägigen Gesetze, Vorschriften und Best Practices der Branche einzuhalten.
* **Sie demonstrieren die Verpflichtung zur Exzellenz:** Organisationen, die sich für die Anwendung dieser Standards und Frameworks entscheiden und sich akkreditieren lassen, zeigen damit ihr Engagement für die Einhaltung hoher professioneller Standards und die Bereitstellung qualitativ hochwertiger Produkte und Dienstleistungen.

#### Inwieweit sind diese Standards und Frameworks untereinander konsistent?

Obwohl jeder Standard und jedes Framework seinen eigenen Schwerpunkt und seine eigene Anwendung hat, teilen sie oft bestimmte Kernprinzipien wie Risikomanagement, Prozessverbesserung und Einhaltung von Vorschriften. Aufgrund dieser Gemeinsamkeiten sind die verschiedenen Normen und Rahmenwerke miteinander kompatibel und ergänzen sich gegenseitig. Beispielsweise können Organisationen problemlos ein Umweltmanagementsystem (ISO/IEC 14001) einführen und dieses nahtlos in ein Arbeitsschutzmanagementsystem (OHSMS) nach OHSAS 18001/ISO/IEC 45001 integrieren. Gleichermaßen können Organisationen, die COBIT für die IT-Governance verwenden, dieses Rahmenwerk mit den ITIL-Praktiken für das Informationssicherheitsmanagement (ISM) abstimmen, um robuste Cybersicherheitsprotokolle zu erhalten. Darüber hinaus folgen diese Standards und Frameworks häufig einer ähnlichen Struktur und nutzen den PDCA-Zyklus (Plan, Do, Check, Act) zur fortlaufenden Verbesserung. Dieser Ansatz ermöglicht es Organisationen, ihren aktuellen Status zu bewerten, Ziele und Vorgaben festzulegen, Maßnahmen umzusetzen und den Fortschritt in den jeweiligen Bereichen des Standards zu überwachen.

Es ist wichtig zu erkennen, dass jeder der oben genannten Standards und Frameworks seinen eigenen Anwendungsbereich, seine eigenen Ziele und spezifischen Anforderungen hat. Organisationen müssen ein tiefes Verständnis für die verschiedenen Aspekte jedes Frameworks entwickeln und wissen, wie sie diese am besten in ihre Geschäftsabläufe integrieren können. Während die Anwendung mehrerer Standards und Frameworks Vorteile bieten kann, kann es auch eine Herausforderung sein, mit überlappenden Bereichen und Anforderungen umzugehen und eine konsistente Anwendung auf allen Ebenen der Organisation sicherzustellen. Unabhängig von den verwendeten Standards oder Frameworks sollten Organisationen stets ein umfassendes Verständnis ihrer Sicherheits-, Compliance- und Risikomanagementanforderungen anstreben. So können sie die geeignete Kombination von Standards und Frameworks auswählen, um ein sicheres Umfeld für Mitarbeitende, Kund:innen und Stakeholder zu schaffen.

### Normen, Gesetze und Verordnungen für Datenschutz und den Schutz der Privatsphäre

In vielen Branchen überschneiden sich die Normen für den Datenschutz und den Schutz der Privatsphäre mit anderen Vorschriften und Rahmenwerken. Die am weitesten verbreiteten Normen für den Datenschutz und den Schutz der Privatsphäre sind von entscheidender Bedeutung, da sie die Anforderungen der Organisation an den Datenschutz und den Schutz der Privatsphäre bei der Erbringung von Dienstleistungen oder der Lieferung von Waren und Produkten festlegen. Die Einhaltung dieser Normen verringert häufig das Risiko von Datenschutzverletzungen und Cyberangriffen und senkt somit effektiv das Risikoniveau der Organisation in Bezug auf Datenschutz und Privatsphäre. Darüber hinaus sind diese Normen und Rahmenwerke von entscheidender Bedeutung für die Implementierung eines ISMS, da sie mit den primären Normen für das umfassende Management der Sicherheitspraktiken der Organisation übereinstimmen:

* **DSGVO (Datenschutz-Grundverordnung):** Die DSGVO ist eine Verordnung, welche die Erhebung, Speicherung, Verarbeitung und Weitergabe personenbezogener Daten von EU-Bürger:innen regelt, unabhängig davon, ob die Organisation ihren Sitz in der EU hat oder nicht. Sie stellt strenge Anforderungen an den Datenschutz, darunter die Notwendigkeit einer ausdrücklichen Einwilligung, Datensicherheitsmaßnahmen und das Recht der Betroffenen auf Löschung ihrer Daten.
* **Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie):** In dieser Richtlinie werden Regeln für die Nutzung elektronischer Kommunikationsmittel wie E-Mail, SMS und Voice-over-IP-Dienste (VoIP) festgelegt. Organisationen müssen die Zustimmung der Nutzer:innen einholen, um deren personenbezogene Daten zu sammeln und zu verwenden, wobei der Verwendungszweck der Daten klar anzugeben ist.
* **Richtlinie über den Datenschutz in der Strafverfolgung:** Dies ist eine Richtlinie für die Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden, die sicherstellen soll, dass die Rechte des Einzelnen gewahrt bleiben und seine personenbezogenen Daten nur für rechtmäßige Zwecke verwendet werden. Diese Richtlinie bezieht sich speziell auf die Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden. Sie stellt sicher, dass die Rechte des Einzelnen gewahrt werden und dass personenbezogene Daten nur für rechtmäßige Zwecke verwendet werden.

Zum Abschluss dieses Lernzyklus sei darauf hingewiesen, dass Normen zum Datenschutz und zum Schutz der Privatsphäre wie die Datenschutz-Grundverordnung, die ePrivacy-Richtlinie und die Richtlinie zum Datenschutz in der Strafverfolgung wichtige Richtlinien darstellen, die Organisationen bei der Verarbeitung sensibler Daten beachten müssen. Die Einhaltung dieser Normen verringert das Risiko von Datenschutzverletzungen und unberechtigtem Datenzugriff und gewährleistet gleichzeitig den Schutz von Unternehmen und Einzelpersonen. Die ordnungsgemäße Umsetzung dieser Normen führt zu einer sicheren Umgebung, die letztendlich das Vertrauen der Kund:innen in die Fähigkeit der Organisation, ihre Daten zu schützen und zu bewahren, stärkt.

### Fragen zur Selbstkontrolle

1. Wie sollten leitende Angestellte die Verwendung internationaler Normen für die Informationssicherheit in einer Organisation sehen?

* *Als Umsetzung einer Best Practice*.
* Wenn das geschäftliche Umfeld stimmt, als eine gute Idee.
* Als Lösung, wenn es eine Sicherheitsverletzung oder ein ernstes Problem in der Organisation gibt.
* Als einzige Aufgabe des IT-Direktors.

1. Bitte vervollständigen Sie den folgenden Satz.

Ein Framework ist bestenfalls ein Rahmen, der als *Vorgehensweise* genutzt werden kann.

## 1.3 Sicherheitsnormen: ISO/IEC 27000-Familie und BSI-Normen

Normen können als Dokumente beschrieben werden, die von international anerkannten Gremien wie der ISO veröffentlicht werden, um die Verbreitung eines gemeinsamen Rahmenwerks zu unterstützen, Sicherheit zu bieten und das Verständnis von Spezifikationen und Prozessen zu fördern, die für die Bereitstellung zuverlässiger Produkte und Dienstleistungen erforderlich sind. Der Zweck von Normen besteht darin, die Herausforderungen zu bewältigen, denen sich Organisationen bei der Bereitstellung von Waren und Dienstleistungen für Verbraucher:innen gegenübersehen. Normen sind spezifische Anforderungen, die übergeordnete Richtlinien unterstützen. (Campbell, 2016). Sie definieren, was eine Organisation tun wird, um ihre politischen Ziele zu erreichen.

### Die ISO/IEC 27000-Normenreihe

Die ISO/IEC 27001 gehört zu einer größeren ISO 27000-Normenfamilie. Sie gilt als Quelle für eine ganze Reihe von Richtlinien, die alle ein weltweit anerkanntes Framework für ein effektives Informationssicherheitsmanagement bieten. Die Normenreihe wurde von einem gemeinsamen Komitee der International Standards Organization (ISO) in Genf und der International Electrotechnical Commission (IEC) entwickelt. Jede Norm der Reihe folgt der Namenskonvention mit einem ISO/IEC-Präfix gefolgt von einem Suffix, welches das Veröffentlichungsdatum angibt. Zum Beispiel wurde ISO 27001:2013 im Jahr 2013 veröffentlicht. Im Laufe der Zeit werden Korrekturen und Aktualisierungen vorgenommen, die das Dokument entsprechend anpassen. Mittlerweile wurde die ISO/IEC 27001:2022 veröffentlicht, die eine Überarbeitung der vorherigen Versionen darstellt. Klauseln sind besondere und separate Artikel, Bestimmungen oder Vorschriften, die in den Normen festgelegt sind. Zum Beispiel ist Klausel 5.2 der ISO/IEC 27001 eine Bestimmung, die von der obersten Leitung einer Organisation verlangt, eine Informationssicherheitspolitik aufzustellen.

**ISO 27001:2013-zertifiziert**

Dies bedeutet, dass das ISMS der Organisation von einer akkreditierten Zertifizierungsstelle nach einem externen Audit für die Konformität mit ISO 27001 zertifiziert wurde.

Wenn eine Organisation **nach ISO 27001:2013 zertifiziert** wurde, muss sie vor der Re-Zertifizierung ein Upgrade auf ISO/IEC 27001:2022 durchführen. Es ist zu beachten, dass je nach Anwendungsbereich des ISMS der Organisation einige neue Maßnahmen eingeführt werden müssen.

Die ISMS-Normenfamilie ist wie folgt gegliedert:

* **die Basisnorm:** ISO/IEC 27000, die als Terminologienorm gilt: Klausel 5.2
* **Anforderungsnormen**: Klausel 5.3 (27001, 27006 und 27009)
* **Leitfadennormen**: Klausel 5.4 (ISO/IEC 27002-8, 270013-14, TR27016, 27021)
* **sektorspezifische Leitfadennormen**: Klausel 5.5 (ISO/IEC 27010-11, 27017-19)
* **maßnahmenspezifische Leitfadennormen:** ISO2703x, ISO2704x

Drei der gängigsten Normen werden im Folgenden beschrieben.

#### Basisnorm: ISO/IEC 27000

Die Basisnorm ISO/IEC 27000 mit dem Titel: *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie*, kann als das Übersichts- und Terminologiedokument bezeichnet werden. Für den Anwendungsbereich bietet dieses Dokument einen Überblick über die ISMS-Normenfamilie, stellt das ISMS, Begriffe und Definitionen vor, die für das ISMS relevant sind.

#### Anforderungsnormen: ISO/IEC 27001

ISO/IEC 27001 mit dem Titel: *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen* ist eine der Normen, die Anforderungen spezifizieren. Wie bereits erwähnt, gibt es innerhalb dieser Kategorie weitere Normen. Im Hinblick auf den Anwendungsbereich spezifiziert die Basisnorm Anforderungen für den Aufbau, die Implementierung, den Betrieb, die Überwachung, die Überprüfung, die Aufrechterhaltung und die Verbesserung des formalisierten ISMS innerhalb einer Organisation. Der Zweck der ISO/IEC 27001 ist es, die normativen Anforderungen für die Entwicklung und den Betrieb eines ISMS innerhalb einer Organisation, unabhängig von deren Größe, Art oder Beschaffenheit, bereitzustellen.

#### Leitfadennormen: ISO/IEC 27002

Ein Beispiel für **Leitfadennormen** ist die ISO/IEC 27002 mit dem Titel: *Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen.* Die ISO/IEC 27002 enthält eine Liste allgemein anerkannter Maßnahmenziele und Best-Practice-Maßnahmen, die als Implementierungsleitfaden für die Auswahl und Umsetzung von Maßnahmen zur Erreichung einer wirksamen Informationssicherheit in einer Organisation dienen. Außerdem enthält dieses Dokument einen Leitfaden für die Umsetzung von Sicherheitsmaßnahmen (insbesondere die Klauseln 5 bis 18), der Organisationen aller Größen, Arten und Umsetzungsformen Ratschläge und Anleitungen zu bewährten Verfahren zur Unterstützung von Sicherheitsmaßnahmen innerhalb der Organisation bietet.

**Leitfaden**

Eine Beschreibung, die verdeutlicht, was und wie etwas getan werden sollte, um die in der Politik festgelegten Ziele zu erreichen.

Im Studienskript wird häufig auf die Norm ISO/IEC 27001:2013 verwiesen. In bestimmten Fällen wird bei Bedarf auch die aktualisierte Version ISO/IEC 27001:2022 erwähnt. Bitte beachten Sie, dass das Weglassen der IEC oder des Suffixes im Namen in diesem Studienskript keinen Einfluss auf die Bedeutung oder die Aussagekraft der Norm hat. Es wird davon ausgegangen, dass die fehlenden Teile implizit sind und dass die Referenz weiterhin den entsprechenden Normen entspricht.

### BSI-Normen

In Deutschland gibt es das Bundesamt für Sicherheit in der Informationstechnik (BSI). Diese Einrichtung ist die oberste Regierungsbehörde, die für die Verwaltung der Computer- und Kommunikationssicherheit zuständig ist. Sie ist auch die zentrale Zertifizierungsstelle für die Sicherheit von IT-Systemen, Computer- und Datensicherheit und Datenschutz in Deutschland. Zu seinen Aufgaben gehören die Sicherung von Computeranwendungen, kritischen Infrastrukturen, Internetsicherheit, Kryptografie sowie die Zertifizierung von Sicherheitsprodukten und die Akkreditierung von Testlabors für Sicherheit in Deutschland. Das BSI gibt Richtlinien heraus, die als BSI-Standards bekannt sind. Sie bieten grundlegende Empfehlungen, technische Anleitungen, Methoden, Prozesse und Verfahren für eine effektive Informationssicherheit in Deutschland. Regierungs- und staatliche Behörden, Unternehmen, Hersteller und Dienstleister nutzen die BSI-Standards. Die BSI-Standards 200-1, 200-2 und 200-3 haben seit Oktober 2017 die BSI-Standards der 100-x-Reihe ersetzt.

#### BSI-Standard 200-x-Reihe

Der BSI-Standard 200-1 definiert die Anforderungen an ein ISMS. Er wurde in Übereinstimmung mit den Anforderungen der ISO/IEC 27001 entwickelt und berücksichtigt gleichzeitig Empfehlungen aus anderen Normen, wie z. B. ISO/IEC 27002.

Der BSI-Standard 200-2 dient als Grundlage für den BSI-Ansatz zum Aufbau eines ISMS mit drei Vorgehensweisen zur Umsetzung des erforderlichen IT-Grundschutzes in einer Organisation. Er erklärt, wie ein ISMS mit Hilfe von drei verschiedenen Methoden aufgebaut werden kann.

Der BSI-Standard 200-3 enthält risikobezogene Schritte und Aufgaben zur Implementierung eines effektiven IT-Sicherheitsrahmens in einer Organisation, um das gewünschte Sicherheitsniveau zu erreichen.

Der BSI-Standard 200-4 ist die modernisierte Norm, die praktische Anleitungen für den Aufbau und die Implementierung von BCM-Systemen (BCM: Business Continuity Management) in einer Organisation enthält.

Aufschlussreich ist, dass die BSI-Standards ideal für Anwender sind, die bereits mit der IT-Grundschutz-Methodik arbeiten und die Risikoanalyse als weitere Ebene hinzufügen wollen.

Die Umstellung auf den modernisierten IT-Grundschutz hat Auswirkungen auf ein ISMS, das auf der bisherigen IT-Grundschutz-Methodik nach dem BSI-Standard BSI 100-2 und den IT-Grundschutz-Katalogen basiert. Dies bedeutet, dass die Umstellung in erster Linie sowohl ISO-zertifizierte als auch nicht zertifizierte Einrichtungen betrifft.

Der Transparenz halber können sich Organisationen nach der ISO/IEC 27001 mit dem IT-Grundschutz als Basis dafür zertifizieren lassen. Diese Art von Zertifikat bestätigt in Deutschland, dass die in der Organisation umgesetzten IT-Sicherheitskonzepte den Anforderungen der weltweit anerkannten Norm ISO/IEC 27001 entsprechen.

### British Standards Institution und BSI-Standards

Die British Standards Institution (BSI-Gruppe), im Folgenden als BSI-UK bezeichnet, ist für die Veröffentlichung von Normen im Vereinigten Königreich (UK) zuständig. Das BSI-UK veröffentlichte erstmals die BS 7799. Die erste Veröffentlichung wurde vom Ministerium für Handel und Industrie der britischen Regierung entwickelt. Im Jahr 1998 wurde der erste Teil, der Best Practices für das Informationssicherheitsmanagement enthielt, überarbeitet. Die ISO hat die BSI-UK-Standards im Jahr 2000 als ISO/IEC 17799 übernommen, die den Titel trägt: „*Informationstechnik –* Leitfaden für das Informationssicherheitsmanagement“. Die neu übernommenen BSI-Standards wurden im Juni 2005 überarbeitet und 2007 als ISO/IEC 27002 in die ISO 27000-Normenfamilie aufgenommen (eine der Normen der Familie, die Leitfäden, genauer Verhaltenskodizes für Informationssicherheitsmaßnahmen beschreibt).

### Fragen zur Selbstkontrolle

1. Der Aufgabenbereich des deutschen BSI umfasst alle folgenden Aufgaben mit Ausnahme von

* *Schutz von Unternehmensnetzwerken, Erkennung und Abwehr von Angriffen auf private Netzwerke.*
* Prüfung, Zertifizierung und Akkreditierung von IT-Produkten und -Dienstleistungen
* Warnung vor Malware oder Sicherheitslücken in IT-Produkten und -Dienstleistungen
* IT-Sicherheitsberatung für die Bundesverwaltung und andere Zielgruppen
* Information und Sensibilisierung der Öffentlichkeit und der Wirtschaft für IT- und Internetsicherheit.

1. Welche der folgenden Organisationen ist für die Pflege von ISO/IEC 27001 verantwortlich?

* *Die Internationale Organisation für Normung*.
* Das Britische Institut für Normung
* Das deutsche Bundesamt für Sicherheit in der Informationstechnik
* Der Normenausschuss der Europäischen Union

## 1.4 Informationssicherheitsmanagementsystem (ISMS)

Ein „Managementsystem“ umfasst alle Maßnahmen innerhalb einer Organisation, die darauf abzielen, die Ziele der Organisation durch Steuerung und Lenkung zu erreichen. Im Bereich der Informationssicherheit wird ein solches System als ISMS bezeichnet. Das ISMS definiert die Werkzeuge und Methoden, die eine Organisation zur Planung, Einführung, Umsetzung, Überwachung und Verbesserung von Sicherheitssystemen einsetzen sollte.

Ein ISMS umfasst in der Regel folgende Hauptkomponenten:

* ISMS-Implementierung und Managementsysteme und -Tools: Für die Umsetzung des ISMS sind die richtigen Prozesse, Systeme und Werkzeuge erforderlich.
* Politiken und Maßnahmen: Politiken und Maßnahmen müssen klar definiert und für alle Stakeholder zugänglich sein.
* Systeme und Tools für das Supply-Chain-Management: Dritte und Lieferanten mit Zugang zu wertvollen Daten müssen verwaltet werden, um die Einhaltung der Vorschriften zu gewährleisten.
* Ressourcen für die Umsetzung: Ein:e klar definierte:r qualifizierte:r Manager:in, ein Team und ein Budget für die Umsetzung des ISMS sind unerlässlich.
* Ressourcen für die fortlaufende Verbesserung: Das ISMS und die Organisation müssen auf Veränderungen aus verschiedenen Quellen, intern und extern, reagieren und sich anpassen.
* Ressourcen für Kommunikation und Einbindung: Die Umsetzung des ISMS erfordert effektive Kommunikation, Einbindung und Sicherheitsschulungen.

Das sind die wichtigsten Komponenten, die für die Implementierung eines ISMS benötigt werden.

Komponenten eines ISMS

Quelle: Andrew Sai (2023).

### Fragen zur Selbstkontrolle

1. Bitte vervollständigen Sie den folgenden Satz.

Um ein ISMS effektiv zu implementieren, sind die folgenden sechs Komponenten erforderlich:Systeme, Tools für die Implementierung und Verwaltung des ISMS, Politiken und Maßnahmen, Systeme und Tools für das Supply-Chain-Management, Ressourcen für die Umsetzung, Ressourcen für die fortlaufende Verbesserung und Ressourcen für Kommunikation und Einbindung.

Zusammenfassung

In dieser Lektion wurden grundlegende Definitionen behandelt, die für das Verständnis von Informationssicherheit und deren Management in einer Organisation wichtig sind. Diese Sicherheitskonzepte sind nach wie vor sowohl für Einzelpersonen als auch für Unternehmen relevant.

Die Gewährleistung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten ist eines der Hauptziele der Informationssicherheit.

Die ISO 27000-Normenfamilie bietet einen geeigneten Rahmen in Form von Best-Practice-Richtlinien für die Implementierung eines ISMS in einer Organisation.

Das ISMS umfasst eine Reihe von Politiken, Maßnahmen und anderen Elementen, die nahtlos in die organisatorischen Prozesse, Verfahren und Praktiken integriert werden sollten.

Es gibt eine Reihe von Normen und regulatorischen Frameworks, die eine direkte Schnittstelle zu den ISMS-Hauptnormen ISO/IEC 27001 und ISO/IEC 27002 haben oder spezifische Branchen abdecken. Es ist wichtig, dass alle diese Normen in den ISMS-Prozess und die Implementierung einbezogen werden, da sie bei Einhaltung zur Schaffung eines sicheren und wachstumsfördernden Umfelds für Organisationen beitragen.

Die erfolgreiche Implementierung eines ISMS bietet Organisationen viele Vorteile, sowohl für die Gegenwart als auch für die Zukunft.

# Lektion 2 – Initiierung eines Informationssicherheitsmanagementsystems

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… können Sie die Prozesse identifizieren und beschreiben, die für die anfängliche Einrichtung des ISMS erforderlich sind.

… sind Sie in der Lage, den Kontext einer Organisation für die ISMS-Implementierung zu analysieren.

… können Sie bestehende ISMS diskutieren, ihren Reifegrad bestimmen und Bereiche für eine fortlaufende Prozessverbesserung ermitteln.

… sind Sie fähig, den Anwendungsbereich des ISMS zu definieren und Sicherheitspolitiken zu formulieren.

# 2. Initiierung eines Informationssicherheitsmanagementsystems

## Einführung

Organisationen verwenden häufig IT-Systeme, um Informationen zu sammeln, zu verarbeiten, zu speichern und zu übertragen. Diese Informationen und Informationswerte sind während ihrer Nutzung anfällig für Angriffe, menschliche und andere Fehler, Naturereignisse und inhärente Schwachstellen.

ISACA (2016), ein Verband für die Prüfung und Kontrolle von Informationssystemen, definiert ein Informationssicherheitsmanagementsystem als „eine umfassende Reihe von Politiken und Prozessen, die eine Organisation einführt und aufrechterhält, um das Risiko für Informationswerte zu managen“ (ISACA, 2016; Übers. d. Autors). Das ISMS soll Organisationen dabei unterstützen, Sicherheitslücken zu erkennen, Sicherheitsvorfälle zu verhindern oder deren Auswirkungen zu minimieren, falls sie dennoch auftreten. Das ISMS dient als zentrale Anlaufstelle für alle Informationen, die für die Gewährleistung der Informationssicherheit in einer Organisation relevant sind.

Das Management der Informationssicherheit innerhalb einer Organisation basiert auf den Vorgaben der ISO 27000-Normenfamilie, insbesondere der ISO/IEC 27001 und 27002, und dient nicht dem Selbstzweck, sondern hat zum Ziel, die Geschäftsprozesse zur Erreichung der Organisationsziele zu unterstützen und den Schutz im Sinne von Vertraulichkeit, Integrität und Verfügbarkeit (CIA) zu gewährleisten.

Diese Lektion behandelt die ersten Schritte zur Vorbereitung der Einführung eines ISMS in einer Organisation.

## 2.1 Ersteinrichtung des ISMS

Die Einrichtung eines ISMS kann aus verschiedenen Gründen erfolgen, sei es, um eine ISO-Zertifizierung zu erlangen oder um gesetzliche Anforderungen zu erfüllen. Bei der Einrichtung eines ISMS müssen Organisationen verschiedene Aspekte berücksichtigen, darunter Governance, Risiko und Compliance. Unabhängig vom Grund der Einrichtung gibt es einige wichtige Bereiche, auf die man sich beim anfänglichen Aufbau und der endgültigen Implementierung eines ISMS in einer Organisation konzentrieren muss.

Die Entwicklung von Richtlinien zur Operationalisierung eines ISMS in Organisationen kann mit verschiedenen Herausforderungen verbunden sein. Insbesondere die Einführung eines zertifizierbaren ISMS in kleinen und mittleren Unternehmen stellt eine Herausforderung dar. Die Implementierung eines ISMS ist ein komplexer Prozess, der mehrere Monate dauern kann und erhebliche Ressourcen erfordert. Für die erfolgreiche Einrichtung eines effektiven ISMS sind in der Regel drei wesentliche Aufgaben zu erfüllen:

**TARA-Framework**

Ein Tool, das Ihnen hilft, Risiken zu bewerten und zu bewältigen. Die Strategien umfassen das Übertragen, Vermeiden, Reduzieren und Akzeptieren von Risiken (Transfer, Avoid, Reduce, Accept).

1. Identifizieren der Informationswerte unter Berücksichtigung der CIA-Triade.
2. Risiken, einschließlich Schwachstellen, Bedrohungen, Szenarien und Wahrscheinlichkeiten beurteilen.
3. Risiken nach dem **TARA-Framework** (Übertragen, Vermeiden, Reduzieren, Akzeptieren) behandeln.

### Fragen zur Selbstkontrolle

1. TARA ist ein Framework, das dabei hilft, Risiken in Organisationen zu bewerten und zu bewältigen. Die Strategien umfassen das *Übertragen*, *Vermeiden*, *Reduzieren* und *Akzeptieren* von Risiken.

## 2.2 Analyse der Organisation

In Übereinstimmung mit den ISO-Normen zum Informationssicherheitsmanagement ist es wichtig, den organisatorischen Kontext zu definieren. Gemäß Klausel 5.3.1 der **ISO/IEC 31000** sollten sowohl interne als auch externe Aspekte beim Aufbau des ISMS berücksichtigt werden.

**ISO 31000**

Hierbei handelt es sich um eine Familie von ISO-Normen, die Grundsätze und allgemeine Richtlinien für das Management von Risiken in einer Organisation enthalten.

Verschiedene ISMS-Praktizierende haben vorgeschlagen, dass es trotz des komplizierten Prozesses möglich ist, die Einführung eines ISMS zu umgehen, indem die folgenden Vorschläge befolgt werden. Es sei darauf hingewiesen, dass es zahlreiche Vorschläge gibt, von denen die folgenden besonders wichtig sind:

### Verständnis des internen organisatorischen Kontextes

Bei der Einrichtung eines ISMS ist das Verständnis des internen Organisationskontextes ein entscheidender Aspekt des Prozesses. Dazu gehört es, Einblicke in die Ziele, Werte, Kultur und Risikotoleranz der Organisation zu gewinnen und ein klares Verständnis der rechtlichen, regulatorischen und vertraglichen Anforderungen zu entwickeln, die für die Informationssicherheit der Organisation gelten. Einige der wichtigsten Faktoren, die in dieser Anfangsphase zu beachten sind, sind die folgenden:

* **Anwendungsbereich und Ziele des ISMS:** Definieren Sie den Anwendungsbereich des ISMS und legen Sie fest, welche spezifischen Bereiche der Organisation abgedeckt werden sollen und welche Ziele das ISMS erreichen soll. So kann das ISMS beispielsweise auf den Schutz von Kundendaten, die Gewährleistung der Geschäftskontinuität oder die Einhaltung bestimmter Vorschriften ausgerichtet sein. Sie haben großen Einfluss auf die Auswahl der Politiken und Verfahren, die in das ISMS aufgenommen werden sollen.
* **Identifizierung und Kommunikation mit den Stakeholdern:** Identifizieren Sie die wichtigen Stakeholder in Ihrer Organisation, wie z. B. Mitarbeitende, Management, Kund:innen und Lieferanten, und berücksichtigen Sie deren spezifische Anliegen und Anforderungen. Binden Sie sie frühzeitig in den Prozess ein, um sicherzustellen, dass ihre Bedürfnisse bei der Gestaltung und Umsetzung des ISMS berücksichtigt werden.
* **Organisationskultur:** Verstehen Sie die Kultur der Organisation, da sie für die erfolgreiche Implementierung eines ISMS entscheidend ist. Dazu gehören Faktoren wie Führungsstile, Entscheidungsprozesse und die allgemeine Einstellung zur Risikobereitschaft. Eine starke Kultur, die der Informationssicherheit einen hohen Stellenwert einräumt, kann zur Wirksamkeit des ISMS beitragen.
* **Ressourcen und Fähigkeiten:** Bewerten Sie die in der Organisation verfügbaren Ressourcen und Fähigkeiten, welche die erfolgreiche Umsetzung des ISMS unterstützen könnten. Dazu gehören sowohl personelle Ressourcen, wie z. B. qualifizierte Informationssicherheitsexpert:innen, als auch finanzielle, technologische und andere Ressourcen. Mögliche Lücken bei den Ressourcen und Fähigkeiten sollten identifiziert werden, um sicherzustellen, dass angemessene Ressourcen zur Unterstützung der ISMS-Implementierung bereitgestellt werden.
* **Gesetzliche, regulatorische und vertragliche Anforderungen:** Identifizieren Sie die gesetzlichen, regulatorischen und vertraglichen Verpflichtungen in Bezug auf die Informationssicherheit, denen die Organisation unterliegt. Dazu gehören Datenschutzgesetze, Cybersicherheitsgesetze und branchenspezifische Anforderungen. Stellen Sie sicher, dass das ISMS diese Anforderungen erfüllt, um die Einhaltung zu gewährleisten und Bußgelder und Strafen zu vermeiden.
* **Risikobereitschaft und -toleranz:** Bewerten Sie die Risikobereitschaft und -toleranz der Organisation im Hinblick auf die Implementierung des ISMS. Dies dient als Leitfaden bei der Auswahl der geeigneten Methoden zur Risikobeurteilung und zum Risikomanagement sowie der Höhe der Investitionen in Maßnahmen zur Informationssicherheit.
* **Überprüfung der bestehenden Politiken, Verfahren und Maßnahmen:** Identifizieren Sie alle bestehenden Politiken, Verfahren und Maßnahmen in Bezug auf die Informationssicherheit. Bewerten Sie deren Wirksamkeit und nutzen Sie diese Informationen als Grundlage für die Entwicklung des ISMS. Dies beinhaltet in der Regel die Aktualisierung oder Ersetzung bestehender Politiken und Verfahren oder die Ergänzung einiger durch zusätzliche Maßnahmen.
* **Integration des ISMS in andere Managementsysteme:** Das ISMS muss mit bestehenden Managementsystemen wie dem Qualitätsmanagementsystem, dem Umweltmanagementsystem oder dem Managementsystem für Gesundheit und Sicherheit am Arbeitsplatz – um nur einige zu nennen – abgestimmt und in diese integriert werden. Dies fördert die Effizienz, reduziert Redundanzen und schafft Synergien zwischen den verschiedenen Systemen. Vergessen Sie nicht, dass das ISMS nicht nur aus einer einzigen Politik besteht, sondern aus einer Reihe von Politiken, Systemen, Prozessen und mehr.

Ein wichtiger Aspekt bei der erstmaligen ISMS-Implementierung ist die Bewertung der Geschäftsanforderungen. Zu verstehen, warum ein Unternehmen existiert, ist entscheidend, um zu beurteilen, was das Unternehmen braucht und um eine geeignete Strategie für die Implementierung von ISO/IEC 27001 zu entwickeln. Aus geschäftlicher Sicht ist dies von entscheidender Bedeutung, und die Geschäftsanforderungen sind eine Teilmenge der internen Kontextanalyse. Wird dieser Schritt übersprungen oder vernachlässigt, kann dies zu Problemen bei der Planung und Analyse des ISMS-Anwendungsbereichs führen, die später im Prozess nur schwer zu beheben sein werden. Es ist wichtig, dies von Anfang an richtig zu machen.

Das Verständnis des internen Geschäftskontextes ist ein entscheidender erster Schritt zur Gestaltung der Organisationskultur und der erfolgreichen Verankerung des ISMS in der Organisation. Dazu gehört auch das Verständnis der Art der Produkte und Dienstleistungen, die den Kund:innen angeboten werden und der mit ihrer Bereitstellung verbundenen Risiken. Aus einer Sicherheitsperspektive werden die Prozesse und Vermögenswerte, die diese Produkte und Dienstleistungen unterstützen und die kontrolliert werden müssen, somit nicht außer Acht gelassen. Dies schließt zudem die Bewertung der Ressourcen ein, die der Organisation zur Prozesssteuerung Verfügung stehen, wie z. B. Technologien, Systeme, Geräte und Personal.

Wenn Sie sich bei der Ersteinrichtung des ISMS Zeit zum Verständnis des internen Organisationskontexts nehmen, können Sie sicherstellen, dass das System auf bestimmte Bedürfnisse zugeschnitten und so konzipiert ist, dass es die organisationsspezifischen Risiken und Herausforderungen effektiv bewältigt. Dies wird letztendlich die Wirksamkeit des ISMS verbessern und dazu beitragen, dass die Organisation ihre Ziele im Bereich der Informationssicherheit erreicht.

### Verständnis des externen organisatorischen Kontexts

Nachdem der interne organisatorische Kontext verstanden wurde, sollte auch der externe Kontext, einschließlich der für die Organisation geltenden Gesetzgebung, betrachtet werden. Dies dient dem Verständnis der Bedrohungen und Risiken, die von der externen Umgebung ausgehen könnten, um so ein wirksames ISMS zu errichten. Dieses Verständnis des externen Kontextes trägt auch zu einer besseren Definition des ISMS-Anwendungsbereichs bei. Anforderungs- und Situationsanalysen sind wichtig für die Definition des ISMS-Anwendungsbereichs.

Der ISMS-Anwendungsbereich ist von entscheidender Bedeutung. Klausel 4.3 der ISO/IEC 27001 legt daher fest, wie dieser zu definieren ist, damit Stakeholder wie Kund:innen, Auditoren, Mitarbeitende der Organisation und die Organisationsleitung wissen, welchen Bereich das ISMS abdeckt.

Einige wichtige zu analysierende Bereiche sind:

* gesetzliche und behördliche Anforderungen, wie z. B. rechtliche, sicherheitstechnische und behördliche Anforderungen, sowie arbeitsrechtliche und IT-bezogene Sicherheitsanforderungen.
* politische und wirtschaftliche Umweltbelange, wie z. B. die Beobachtung von Änderungen der Regierungspolitik und von Wechselkursschwankungen, zusammen mit anderen Wirtschaftsindikatoren und sozialen Belangen.

### Erstellung einer Informationssicherheitspolitik

Sobald der interne und externe organisatorische Kontext klar verstanden wurde, liegt es in der Verantwortung der **obersten Leitung**, eine Informationssicherheitspolitik gemäß den Anforderungen von Klausel 5.2 der ISO 27001 festzulegen. Die Informationssicherheitspolitik muss in einem dokumentierten Format vorliegen. Das bedeutet, dass die oberste Leitung das Dokument erstellen und sicherstellen muss, dass es für alle relevanten Parteien zugänglich und relevant ist. Die Politik muss vom Vorstand genehmigt und veröffentlicht werden, damit wichtige Stakeholder wie Mitarbeitende, Kund:innen und Lieferanten Kenntnis davon nehmen können. Das Dokument zur Informationssicherheitspolitik sollte klar definieren, welche Ziele das ISMS erreichen soll.

**Oberste Leitung**

Die Personen, die eine Organisation leiten und kontrollieren.

Die Festlegung einer Informationssicherheitspolitik ist ein entscheidender Schritt zur Implementierung eines effektiven ISMS gemäß der ISO/IEC 27001. Die Politik bildet die Grundlage für den risikobasierten Ansatz der Organisation und trägt zur Förderung einer Kultur des Sicherheitsbewusstseins und der Verantwortlichkeit bei. Um sicherzustellen, dass Informationssicherheitsrichtlinien umfassend und solide sind, sollten Organisationen Faktoren wie die Managementeinbindung, die Ausrichtung nach den Organisationszielen, einen risikobasierten Ansatz, klare Rollen und Verantwortlichkeiten, fortlaufende Verbesserung, effektive Kommunikation, Vorfallsmanagement, Geschäftskontinuität sowie Überprüfung und Aktualisierung berücksichtigen. Im Folgenden finden Sie eine Übersicht über die bei der Erstellung einer Informationssicherheitspolitik gemäß der ISO/IEC 27001 zu beachtenden Punkte. Einige der zu überprüfenden Punkte auf der Liste sind, dass die Informationssicherheitspolitik mit den Zielen der Organisation übereinstimmen sollte und dass die Rollen und Verantwortlichkeiten klar definiert sein sollten, was später in dieser Lektion behandelt wird. Einige der wichtigsten Aspekte sind die folgenden:

* **Engagement des Managements und Top-Down-Ansatz:** Organisationen müssen sich auf höchster Ebene engagieren, d. h. die erforderlichen Ressourcen bereitstellen, organisatorische Prioritäten setzen und eine sicherheitsbewusste Kultur fördern. Die Geschäftsleitung sollte ein interdisziplinäres Team von Stakeholdern einsetzen, um die Informationssicherheitspolitik zu entwickeln und aufrechtzuerhalten.
* **Abstimmung mit den Zielen und rechtlichen Anforderungen:** Diese Abstimmung der Informationssicherheitspolitik auf die strategischen Ziele, die rechtlichen und regulatorischen Anforderungen und die Risikobereitschaft der Organisation ist wichtig, um sicherzustellen, dass die Politik relevant ist und den Sicherheitsanforderungen der Organisation entspricht. Daher ist es wichtig, alle relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen in Bezug auf Informationssicherheit, Datenschutz und Datensicherheit zu identifizieren und deren Einhaltung zu gewährleisten.
* **Risikobasierter Ansatz:** ISO/IEC 27001 befürwortet einen risikobasierten Ansatz für das Informationssicherheitsmanagement. Daher sollte eine solide Informationssicherheitspolitik auf einer umfassenden Risikobeurteilung basieren, bei der Bedrohungen und Schwachstellen, die sich auf Informationswerte auswirken können, identifiziert und bewertet werden. Organisationen können Ressourcen effizienter einsetzen und Maßnahmen effektiver durchführen, wenn Schritte zur Risikominderung nach ihrer Wahrscheinlichkeit und ihren potenziellen Auswirkungen priorisiert werden.
* **Grundlegende Maßnahmen und fortlaufende Verbesserung:** ISO/IEC 27001:2013 bietet einen Katalog von 114 Maßnahmen in 14 Maßnahmenbereichen, der als Anhang A bezeichnet wird. Diese Maßnahmen dienen als Ausgangspunkt für Organisationen, um ihre eigenen grundlegenden Sicherheitsmaßnahmen auf der Grundlage ihres Risikobeurteilungsprozesses zu entwickeln. In einer Informationssicherheitspolitik sollten die grundlegenden Sicherheitsmaßnahmen festgelegt und die Verfahren für ihre Umsetzung, Überwachung und Pflege geklärt werden. Außerdem sollte die Politik einen fortlaufenden Verbesserungsprozess durch regelmäßige Überprüfung, Überwachung und Bewertung der Wirksamkeit des ISMS fördern.
* **Kommunikationsstrategie:** So wird sichergestellt, dass die Informationssicherheitspolitik von allen Stakeholdern verstanden und angenommen wird. Regelmäßige Kommunikation und Feedback-Mechanismen sorgen für ein einheitliches Verständnis der Informationssicherheitspolitik.

### Rollen und Verantwortlichkeiten – Definitionen

Die Einbindung und Zustimmung des Managements ist ein wichtiger Schritt auf dem Weg zur Implementierung des ISMS. Die Zustimmung zeigt, dass das ISMS von der Spitze der Organisation gesteuert wird. Ein weiterer Schritt ist die Definition von Rollen, Verantwortlichkeiten und Kompetenzen. Die Norm ISO/IEC 27001 definiert in Klausel 5.3 die erforderlichen Rollen, Verantwortlichkeiten und Kompetenzen. Die Organisation muss diese Rollen definieren, um das Informationssicherheitsmanagementsystem (ISMS) effektiv zu implementieren. Es ist wichtig, für jede definierte Rolle klare Verantwortlichkeiten für die Einführung, Pflege und fortlaufende Verbesserung des ISMS festzulegen. Insbesondere die Führungsebene und die oberste Leitung spielen in diesem Schritt eine wichtige Rolle. Ohne das Engagement der obersten Leitung wird ein ohnehin schon anspruchsvoller Prozess noch komplexer.

Die Implementierung eines ISMS erfordert die Zuweisung spezifischer Rollen und Verantwortlichkeiten, um eine effektive Steuerung und Kontrolle der Informationssicherheit zu gewährleisten. Nachfolgend werden einige der wichtigsten Aufgaben beschrieben, die gemäß ISO/IEC 27001 für ein ISMS erforderlich sind.

#### Oberste Leitung

Die oberste Leitung gibt die allgemeine Richtung für die Informationssicherheitsmaßnahmen der Organisation vor und stellt sicher, dass die notwendigen Ressourcen für die Umsetzung des ISMS bereitgestellt werden. Wichtige Aufgaben sind

* die Festlegung der ISMS-Politik.
* die Sicherstellung der Einhaltung gesetzlicher und regulatorischer Anforderungen.
* die Unterstützung bei der Gestaltung, Umsetzung und Verbesserung des ISMS und
* die Überprüfung der Wirksamkeit des ISMS.

#### Chief Information Security Officer (CISO)

Der CISO ist für die Überwachung des gesamten Informationssicherheitsprogramms verantwortlich und stellt sicher, dass die Sicherheitsmaßnahmen in allen Bereichen der Organisation integriert sind. Die Aufgaben des CISO umfassen:

* Sicherstellung der Konformität der Richtlinien und Verfahren mit den Zielen der Organisation und den Anforderungen der ISO-Normen.
* Koordination mit den relevanten Stakeholdern, um sicherzustellen, dass diese über das Informationssicherheitsmanagementsystem (ISMS) und dessen Leistung informiert sind.
* Überwachung von Sicherheitsrisiken und regelmäßige Aktualisierung des ISMS
* Überwachung der Reaktion auf Sicherheitsvorfälle und Berichterstattung darüber.

#### Data Protection Officer (DPO)

Der DPO (Datenschutzbeauftragter) überwacht die Datenschutzangelegenheiten der Organisation und stellt sicher, dass die Datenschutzbestimmungen eingehalten werden. Zu den wichtigsten Aufgaben des DPO gehören:

* gründliche Kenntnis der Datenschutzgesetze und -vorschriften
* Beratung zu Datenschutzanforderungen und potenziellen Risiken für den Datenschutz
* Sicherstellung der Durchführung von Datenschutz-Audits
* Unterstützung von Datenschutzschulungen und Sensibilisierungsinitiativen

#### ISMS-Manager

Diese:r Manager:in ist für die tägliche Verwaltung und Pflege des ISMS verantwortlich. Er/Sie hat folgende Aufgaben:

* Sicherstellung, dass das ISMS effektiv umgesetzt und gepflegt wird.
* Koordinierung mit den wichtigsten Stakeholdern, um zu gewährleisten, dass sie ihre Rollen in Bezug auf das ISMS verstanden haben.
* Überprüfung und Aktualisierung des ISMS, um sicherzustellen, dass es wirksam bleibt und den Anforderungen der ISO/IEC 27001 entspricht.
* Beratung und Unterstützung bei ISMS-Audits und -Beurteilungen.

#### Computer Emergency Response Team (CERT)

Dieses Team ist für die Bearbeitung und Reaktion auf Sicherheitsvorfälle verantwortlich, um deren effektive Lösung zu gewährleisten. Seine Hauptaufgaben sind u. a.:

* Überwachung der Informationssysteme auf potenzielle Sicherheitsvorfälle.
* Identifizieren, Analysieren und Reagieren auf Sicherheitsvorfälle.
* Kommunikation mit den betroffenen Parteien und Koordinierung der Reaktion auf den Vorfall.
* Dokumentation und Berichterstattung über Sicherheitsvorfälle einschließlich der daraus gewonnenen Erkenntnisse zur Verbesserung der ISMS-Prozesse.

Um die Rollen und Verantwortlichkeiten klarer zu definieren, kann eine RACI-Matrix (Responsible, Accountable, Consulted, Informed) verwendet werden. Eine RACI-Matrix für die oben genannten Rollen könnte wie folgt aussehen:

Beispiel einer RACI-Matrix für ISMS-Rollen und -Verantwortlichkeiten

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rolle/Verantwortung | Oberste Leitung | CISO | DPO | ISMS-Manager | CERT |
| ISMS-Politik einführen | A | C | C | R | I |
| Einhaltung von Gesetzen sicherstellen | A | R | R | C | I |
| Wirksamkeit des ISMS überprüfen | A | C | I | R | I |
| Mit Stakeholdern koordinieren | R | A | R | R | I |
| Risiken überwachen und ISMS aktualisieren | I | A | C | R | R |
| Auf Vorfälle reagieren und Bericht erstatten | I | R | I | C | A |

Quelle: Andrew Sai (2023)

### Risikobeurteilung

Klausel 6 der ISO/IEC 27001 legt fest, dass Organisationen das Risiko bewerten und Maßnahmen zum Umgang mit Informationssicherheitsrisiken gemäß den folgenden Schritten entwickeln müssen:

1. Planung: In dieser Phase wird der Prozess der Risikobeurteilung vereinbart und die identifizierten, beurteilten und behandelten Risiken werden dokumentiert. Signifikante Risiken werden identifiziert, gewichtet und bewertet. Diese erste Phase ist in Klausel 6.1.1 unter „Planung“ der ISO/IEC 27001 beschrieben.
2. Risikobeurteilung: In diesem Schritt wird eine Methodik für die Risikobeurteilung festgelegt, angewendet und entsprechend dokumentiert. Gemäß Klausel 6.1.2 sollte der Risikobeurteilungsprozess:
   1. Risikokriterien für die Informationssicherheit definieren und pflegen können.
   2. Wiederholte Risikobeurteilungen sollten konsistent, gültig und vergleichbar sein.
   3. In der Lage sein, Risiken im Zusammenhang mit Verlusten aufgrund von Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit im Rahmen des ISMS zu identifizieren.
   4. Klare Verantwortlichkeiten für die Risiken festlegen.
   5. Informationssicherheitsrisiken nach festgelegten Kriterien beurteilen können.
3. Dokumentation: Der gesamte Prozess der Beurteilung von Informationssicherheitsrisiken sollte dokumentiert werden.
4. Risikobehandlung: Nach Abschluss der Risikobeurteilung sollte ein Risikobehandlungsplan entwickelt werden. Dieser Plan beschreibt die erforderlichen Schritte, um die Auswirkungen der identifizierten Risiken zu mindern und mit den Restrisiken umzugehen. Zu den verfügbaren Optionen für die Behandlung gehören die Übertragung, Vermeidung, Verringerung oder Akzeptanz von Informationssicherheitsrisiken (TARA).
5. Risikomaßnahmen: Nach der Erstellung des Risikobehandlungsplans müssen die zu ergreifenden Maßnahmen festgelegt werden. Anhang A der ISO/IEC 27001:2013 beschreibt 114 Maßnahmen, die in 14 Gruppen unterteilt sind. Es ist wichtig zu beachten, dass Organisationen nicht verpflichtet sind, alle in Anhang A aufgeführten Maßnahmen vollständig umzusetzen, sondern nur diejenigen, die nach der Risikobeurteilung relevant sind.

Im Rahmen der Risikobehandlungsschritte ist gemäß Klausel 6.1.3d der ISO/IEC 27001:2013 eine Erklärung zur Anwendbarkeit (Statement of Applicability, SoA) auszufüllen. Die SoA zeigt auf, welche Maßnahmen implementiert sind und die Gründe hierfür, sowie welche Maßnahmen nicht implementiert sind – ebenso mit Begründung. Gemäß dem ISO/IEC 27001 **Technischen Korrigendum** 2 muss die von Organisationen erstellte SoA folgende Informationen enthalten: die vorhandenen erforderlichen Maßnahmen, die Begründung für ihre Implementierung, die Implementierung dieser Maßnahmen und die Begründung für den Ausschluss von Maßnahmen, die in Anhang A der ISO/IEC 27001 aufgeführt sind. Es ist zu beachten, dass diese Anforderungen in der Version ISO/IEC 27001:2022 aktualisiert wurden.

**Technisches Korrigendum**

Diese werden herausgegeben, um technische Fehler oder Unklarheiten in den Normen zu berichtigen, die versehentlich bei der Erstellung oder beim Druck der Veröffentlichung aufgetreten sind. Sie werden jedoch nicht für Fehler ausgestellt, von denen angenommen wird, dass sie keine Auswirkungen auf die Anwendung der Veröffentlichung haben.

### Durchführung eines internen Audits

Organisationen sind gemäß Klausel 9.2 der ISO/IEC 27001:2013 verpflichtet, regelmäßig interne Audits durchzuführen, um zu beurteilen, ob die Umsetzung des ISMS den organisatorischen Anforderungen und Standards entspricht. Eine unabhängige Überprüfung des ISMS durch einen kompetenten Auditor ist von entscheidender Bedeutung, unabhängig davon, ob es sich um eine interne oder externe Organisation handelt. Es ist wichtig, dass der Auditor, der das Audit durchführt, nicht an der Umsetzung des ISMS beteiligt ist. Es wird empfohlen, dass diese unabhängige Prüfung von einem erfahrenen ISO/IEC 27001-Auditor oder einem zertifizierten Unternehmen durchgeführt wird.

Das interne Audit ist ein systematischer, unabhängiger und dokumentierter Prozess zur Bewertung und Beurteilung der Wirksamkeit des ISMS der Organisation gemäß ISO/IEC 27001. Es dient dazu, Nichtkonformitäten, Lücken und Verbesserungsmöglichkeiten im ISMS aufzudecken. Der Umfang solcher Audits umfasst alle Aspekte des ISMS, einschließlich der Politiken, Verfahren, Maßnahmen, Risikobeurteilungen und der allgemeinen Sicherheitslage der Organisation. Das interne Audit wird entweder von internen Auditoren oder gegebenenfalls von externen Fachleuten durchgeführt. Diese Auditoren sind in der Regel unabhängig von der täglichen Verwaltung des ISMS. Die Ergebnisse des internen Audits werden an die oberste Leitung der Organisation oder an relevante Stakeholder berichtet.

### Managementbewertung

Das Management einer Organisation, die ein ISMS einführt, ist für die Durchführung einer Managementbewertung gemäß ISO/IEC 27001 verantwortlich. Diese Bewertung muss im Voraus geplant werden und soll sicherstellen, dass das ISMS wirksam ist und zur Erreichung der Unternehmensziele beiträgt. Die Managementbewertung wird als letzter Schritt in der Prozesskette angesehen.

Die Managementbewertung ist eine regelmäßige Bewertung des ISMS durch die oberste Leitung der Organisation, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit bei der Erfüllung der Sicherheitsziele der Organisation und der Anforderungen der ISO/IEC 27001 Norm zu beurteilen.

Der Zweck der Managementbewertung ist es, fundierte Entscheidungen über das ISMS zu treffen und Ressourcen für die fortlaufende Verbesserung bereitzustellen. Es beinhaltet eine hochrangige Überprüfung des ISMS mit Schwerpunkt auf Zielen, Ergebnissen, Ressourcenzuweisung und Gesamtleistung. Beteiligte Parteien sind die oberste Leitung oder deren Vertreter:innen, in der Regel unterstützt durch den/die ISMS-Manager:in, den CISO oder relevante Stakeholder.

Um die Managementbewertung von der internen Revision zu unterscheiden, sind die Ziele, der Umfang und die Teilnehmer:innen zu beachten. Das interne Audit ist eine detailliertere Bewertung, die sich auf die Identifizierung von Nichtkonformitäten und Verbesserungsmöglichkeiten konzentriert, während die Managementbewertung eine Bewertung des ISMS auf hoher Ebene ist, um sicherzustellen, dass es wirksam bleibt und den Zielen der Organisation entspricht. Schließlich wird das interne Audit von unabhängigen Wirtschaftsprüfer:innen durchgeführt, während die Managementbewertung von der obersten Leitung durchgeführt wird.

### Fragen zur Selbstkontrolle

1. Die Implementierung eines Systems zur Gewährleistung der Informationssicherheit sollte innerhalb einer Organisation als… betrachtet werden.

* ein Problem der IT-Abteilung
* ein Problem der Führungsebene
* ein Problem für externe Expert:innen
* *ein Problem für die gesamte Organisation*

1. Bitte nennen Sie drei Prozesse in den Schritten, die bei der Einrichtung eines ISMS analysiert und berücksichtigt werden sollten.

*Den internen organisatorischen Kontext verstehen*

*Den externen organisatorischen Kontext verstehen*

*Erstellung einer Informationssicherheitspolitik*

*Definition von Rollen und Verantwortlichkeiten*

*Risikobeurteilung*

*Durchführung von internen Audits*

*Managementbewertung*

## 2.3 Analyse des bestehenden ISMS und Bestimmung des Reifegrads

Der Reifegrad eines ISMS bezieht sich auf seinen Entwicklungsstand, seine Wirksamkeit und seine Anpassungsfähigkeit an sich wandelnde Bedrohungen und Geschäftsanforderungen. In diesem Lernzyklus werden einige typische Faktoren erörtert, die bei der Bewertung eines bestehenden ISMS zur Bestimmung seines Reifegrads zu berücksichtigen sind, sowie einige häufig verwendete Reifegradmodelle.

### Zu berücksichtigende Faktoren bei der Bewertung des ISMS-Reifegrades

Die Bewertung des Reifegrads eines ISMS ermöglicht es Organisationen, Bereiche mit Verbesserungspotenzial zu identifizieren, Investitionen zu priorisieren und den Stakeholdern den Fortschritt aufzuzeigen. Es gibt viele Faktoren, die bei der Bewertung des Reifegrads eines ISMS berücksichtigt werden sollten, damit das ISMS nicht nur die Sicherheit der Organisation verbessert, sondern auch die Einhaltung von Vorschriften, Standards und Best Practices der Branche gewährleistet. Die Liste der zu berücksichtigenden Faktoren ist lang und umfasst unter anderem den Ansatz einer Organisation für interne und externe Audits, die Integration des ISMS in andere Managementsysteme, die Sicherheit von Dritten und der Lieferkette, die Einhaltung gesetzlicher und behördlicher Anforderungen, das effektive Management von Sicherheitsvorfällen, klare Rollen und Verantwortlichkeiten für die Informationssicherheit in der Organisation, die Mitarbeiterschulung und -sensibilisierung sowie die fortlaufende Verbesserung durch einen strukturierten Überprüfungsansatz und die Leistungsüberwachung des bestehenden ISMS.

* **Überprüfung des ISMS-Frameworks und der Politikumsetzung**: Dies ist oft der erste Schritt bei der Analyse eines bestehenden ISMS und beinhaltet die Überprüfung des Anwendungsbereichs, der Ziele und der Politiken des ISMS, sodass sie mit den Zielen der Organisation übereinstimmen und die Risiken der Informationssicherheit angemessen berücksichtigen. Die Durchsetzung, Kommunikation und Aktualisierung von Politiken zur Berücksichtigung von Veränderungen in der Bedrohungslandschaft und im Geschäftsumfeld ist ein Indikator für den Reifegrad des ISMS.
* **ein solides Verfahren für die Risikobeurteilung und das Risikomanagement**: Eine wirksame Risikobeurteilung und ein wirksames Risikomanagement sind für die Identifizierung und Minderung von Risiken von entscheidender Bedeutung. Dieser Prozess sollte transparent, wiederholbar und an die Risikobereitschaft der Organisation angepasst sein. Die Bewertung der bestehenden Risikobeurteilungsmethode kann helfen, den Reifegrad des ISMS zu bestimmen. Ein ausgereiftes ISMS verwendet einen systematischen Ansatz, um Risiken zu identifizieren, zu analysieren und zu priorisieren. Anschließend werden geeignete Risikobehandlungen und Maßnahmen implementiert, um die Risiken auf einem akzeptablen Niveau zu halten.
* **Kennzahlen und Leistungsindikatoren**: Wenn eine Organisation in der Lage sein soll, den Erfolg und den Reifegrad eines ISMS zu messen, müssen relevante Kennzahlen und Leistungsindikatoren festgelegt werden. Zu diesen Kennzahlen könnten die Anzahl der Sicherheitsvorfälle, die Zeit bis zur Entdeckung von Vorfällen und die Reaktion darauf, die Abschlussquote der Mitarbeiterschulungen und die Wirksamkeit der Risikomanagementmaßnahmen gehören.
* **Informationssicherheitskultur**: Die Sicherheitskultur innerhalb einer Organisation hat einen erheblichen Einfluss auf den Gesamtreifegrad eines ISMS. Ein ausgereiftes ISMS fördert eine proaktive Sicherheitskultur, in der Sicherheitsaspekte regelmäßig von der Führungsebene kommuniziert werden. Wirksame Schulungs- und Sensibilisierungsprogramme für das Personal tragen zur Schärfung des Bewusstseins für Sicherheitsfragen bei. Darüber hinaus wird die Integration von Sicherheitsüberlegungen in die täglichen Entscheidungsprozesse gefördert.

Die Bewertung des Reifegrads des ISMS einer Organisation ist von großer Bedeutung, um die allgemeine Sicherheit und den Schutz von Informationswerten zu verbessern. Durch die Berücksichtigung der oben genannten Faktoren können Organisationen wertvolle Erkenntnisse über die Stärken und Schwächen ihres ISMS gewinnen. Identifizierte Schwachstellen können entsprechend priorisiert und verbessert werden, um einen optimalen Reifegrad des ISMS zu erreichen.

### Reifegradmodelle

Reifegradmodelle unterstützen Organisationen bei der Beurteilung ihres ISMS-Reifegrades. Sie dienen als Benchmarking-Instrument, mit dem Organisationen ihre Fortschritte im Vergleich zu anderen Organisationen messen und auf der Grundlage bewährter Praktiken ermitteln können, welche Elemente sie implementieren sollten. Durch die Verwendung dieser Modelle zur Bewertung des ISMS wird die Übernahme von Best Practices gefördert. Ein zentraler Aspekt, der in den ISMS-Reifegradmodellen hervorgehoben wird, ist die Bedeutung einer Sicherheitskultur für den Schutz der Informationswerte einer Organisation.

Es gibt verschiedene bekannte Reifegradmodelle, von denen einige fünf und andere sechs Stufen verwenden. Unabhängig von der Anzahl der Stufen in einem bestimmten Modell besteht das gemeinsame Ziel darin, ähnliche oder identische Ziele zu erreichen.

#### NIST CSEAT IT Security Maturity Model

Dieses Modell umfasst fünf progressive Reifegrade, die sich auf die Dokumentation konzentrieren. Die fünf Reifegrade sind (NIST, 2016):

1. Politiken
2. Verfahren
3. Implementierung
4. Test
5. Integration

**Citigroups Information Security Evaluation Model (CITI-ISEM)**

Dieses Modell besteht aus fünf progressiven Reifegraden, wobei der Schwerpunkt auf dem organisatorischen Bewusstsein und der Übernahme liegt. Die fünf Reifegrade sind (Citigroup, 2000):

1. Selbstzufriedenheit
2. Anerkennung
3. Integration
4. Übliche Praxis
5. Fortlaufende Verbesserung

#### COBIT-Reifegradmodell

Das COBIT-Reifegradmodell hat sechs progressive Reifegrade, die sich auf die Prüfung spezifischer Verfahren konzentrieren. Die sechs Reifegrade (beginnend bei Null) sind (CEWebS, 2009):

1. Nicht vorhanden
2. Erstmalig/Ad-hoc
3. Wiederholbar, aber intuitiv
4. Definierter Prozess
5. Verwaltet und messbar
6. Optimiert

#### Systems Security Engineering Capability Maturity Model (SSE-CMM)

Dieses Modell besteht aus sechs Reifegraden, die sich auf die Messung von Sicherheitstechnik und Softwaredesign konzentrieren. Es dient als allgemeines Framework für die Durchführung von Security Engineering innerhalb einer Organisation. Die ISO/IEC 21827:2008 empfiehlt das SSE-CMM zur Beschreibung wesentlicher Merkmale von Security-Engineering-Prozessen für Organisationen. Die sechs Reifegrade, beginnend mit Stufe 0 als der am wenigsten entwickelten Reifegradstufe, sind (ISO, 2008):

1. Nicht durchgeführt
2. Informell durchgeführt
3. Geplant und nachverfolgt
4. Gut definiert
5. Quantitativ kontrolliert
6. Fortlaufend verbessert

#### CERT/CSO Security Capability Assessment

Dieses Modell umfasst fünf progressive Reifegrade, die sich auf die Dokumentation konzentrieren. Die fünf Reifegrade sind:

1. Vorhanden
2. Wiederholbar
3. Benannte Person
4. Dokumentiert
5. Überprüft und aktualisiert

### ISMS-Reifegradbeurteilungsmethodik – Phasen

Auf der Grundlage der ISO/IEC 27001-Normen sind Organisationen, die ein ISMS eingeführt haben, verpflichtet, dessen Wirksamkeit zu messen und das ISMS kontinuierlich zu verbessern. Für die Messung der Leistung eines ISMS gibt es keine standardisierte, ganzheitliche Methodik. Allerdings bieten Best Practices und die Vorschriften der Normen praktische Methoden für die Durchführung einer Reifegradbewertung. Während die ISO/IEC 27001 Konformitätsanforderungen festlegt, bietet die ISO/IEC 27002 Richtlinien, die bei der Entwicklung eines ISMS und der Implementierung von ISMS Best Practices helfen. Vor diesem Hintergrund sind die Phasen der ISMS-Reifegradbeurteilungsmethodik wie folgt (Monev, 2020).

#### Phase 1: Einleitung der Beurteilung

Eine kompetente Person sollte die Beurteilung eines bestehenden ISMS einleiten. Diese Person sollte sich die Unterstützung der obersten Führungsebene und anderer Abteilungen und Stakeholder sichern und die Grundlagen für eine fortlaufende Beurteilung des ISMS-Reifegrads schaffen.

#### Phase 2: Ernennung eines Beurteilungsteams

In der zweiten Phase der Beurteilung des bestehenden ISMS sollte ein Beurteilungsteam ernannt werden. In der Regel sollte das Team aus Expert:innen für Informationssicherheit und Compliance bestehen. Externe Berater:innen können bei Bedarf hinzugezogen werden, und als Empfehlung ist ein formelles Mandat des Managements für die Beurteilung erforderlich.

#### Phase 3: Erstellung von Beurteilungsinstrumenten

Ein Beurteilungstool für das bestehende ISMS ist der nächste Schritt, und ein solches sollte erstellt werden. Dies wird häufig über Microsoft Excel-Vorlagen oder andere kommerziell erhältliche Vorlagen verwaltet. Für die ISO/IEC 27001-Maßnahmen (114 im Anhang A der ISO/IEC 27001:2013), zusammen mit den 25 Unterklauseln (insgesamt etwa 139), wird das Beurteilungstool in der ISMS-Bewertung zur Informationseingabe verwendet und bleibt das Hauptdokument des Abschlussberichts über den ISMS-Reifegrad.

#### Phase 4: Überprüfung von Dokumenten und Interviews

In Übereinstimmung mit dem Leitfaden für Best Practices sollten die relevanten Dokumente zur Informationssicherheit in der Organisation und andere Informationsquellen überprüft werden. Es sollten Interviews mit Einzelpersonen in Bezug auf etablierte Prozesse durchgeführt werden, um ein besseres Verständnis der Verfahren mit reduziertem Reifegrad zu erhalten und die aktuelle Situation der Sicherheitsmaßnahmen zu beschreiben.

#### Phase 5: Bewertung und Empfehlungen

Es wird empfohlen, während der Überprüfung der Dokumente und der Interviews den Reifegrad jeder einzelnen der 139 Maßnahmen (soweit es sich um die ISO/IEC 27001:2013 NS 27002:2013 handelt) anhand einer Skala zu bewerten, die auf einer Reifegrad-Referenztabelle basiert. Für jede Maßnahme können Empfehlungen ausgesprochen werden, nachdem die ISO/IEC 27002 sowie andere Referenzen und Best Practices konsultiert wurden.

#### Phase 6: Berichterstattung

Es wird empfohlen, die Reifegradbeurteilung mit einem Beurteilungsbericht abzuschließen, der die Kennzahlen über die Leistung des bestehenden ISMS enthält. Ein Abschnitt sollte den Grad der Übereinstimmung mit der ISO/IEC 27001 abdecken. Der Beurteilungsbericht sollte auch eine Erläuterung der Beurteilungsergebnisse enthalten, die sich auf die durchgeführten Interviews, die Auswertung der Dokumente und die Empfehlungen zur Verbesserung des bestehenden ISMS konzentrieren.

### Fragen zur Selbstkontrolle

1. Die ISO/IEC 27001 bietet Richtlinien für die Gestaltung eines ISMS und die Umsetzung bewährter ISMS-Verfahren, während die ISO/IEC 27002 Konformitätsanforderungen enthält. Richtig oder Falsch?

* Richtig
* *Falsch*

1. Nennen Sie bitte drei bekannte Reifegradmodelle für die Informationssicherheit.

*NIST CSEAT IT Security Maturity Model*

*Citigroups Information Security Evaluation Model*

*(CITI-ISEM)*

*COBIT-Reifegradmodell*

*Systems Security Engineering Capability Maturity Model*

*(SSE-CMM)*

*CERT/CSO Security Capability Assessment*

## 2.4 Definition des Anwendungsbereichs des ISMS und der Sicherheitspolitiken

Die Festlegung des Anwendungsbereichs sollte frühzeitig erfolgen, in der Regel im Rahmen der erstmaligen Einführung des ISMS, und kann dann iterativ angepasst werden.

Die Grenzen und die Eignung des ISMS bilden seinen Anwendungsbereich. Bei der Festlegung des Anwendungsbereichs sollten der interne und externe Kontext, die Ergebnisse der Anforderungsanalyse gemäß Klausel 4.1 der ISO/IEC 27001:2013, die Schnittstellen und Abhängigkeiten zwischen den internen und externen Aktivitäten einer Organisation sowie andere Faktoren, welche die Festlegung des Anwendungsbereichs beeinflussen können, sorgfältig geprüft werden. Die Dokumentation des Anwendungsbereichs sollte als formale Aufzeichnung verfügbar sein (Hintzbergen et al., 2015).

Der Anwendungsbereich kann alle Teile der Organisation umfassen. Wenn der Anwendungsbereich des ISMS jedoch auf einen bestimmten Teil der Organisation beschränkt ist, sollten klare Grenzen definiert werden. Das Management sollte auf der Grundlage der Unternehmensziele und der Gründe für die Auswahl des ISMS-Bereichs über den Umfang des Anwendungsbereichs entscheiden. Dies kann die Aktivitäten einer Geschäftseinheit, einer Abteilung, eines Projekts oder einer bestimmten Funktion oder Dienstleistung umfassen, wie in der folgenden Abbildung dargestellt.

ISMS-Anwendungsbereich – Szenarien

Diagramm

Beschreibung automatisch generiert

Quelle: Andrew Sai (2023).

### Ziel der Definition des ISMS-Anwendungsbereichs

Ein wohldefinierter ISMS-Anwendungsbereich bietet mehrere Vorteile. Organisationen, die den spezifischen Anwendungsbereich des ISMS festlegen und implementieren, erreichen folgende Ziele:

* Minimierung der geschäftlichen Auswirkungen und finanziellen Kosten von Sicherheitsvorfällen in einem oder mehreren Geschäftsbereichen
* Verringerung der Anzahl und Häufigkeit von Sicherheitsvorfällen
* Einhaltung von Gesetzen und Vorschriften wie den Datenschutzrichtlinien der Europäischen Union (EU), den SOX- oder HIPAA-Vorschriften in den USA
* Förderung des Unternehmenswertes und Schaffung eines Business-Enablers

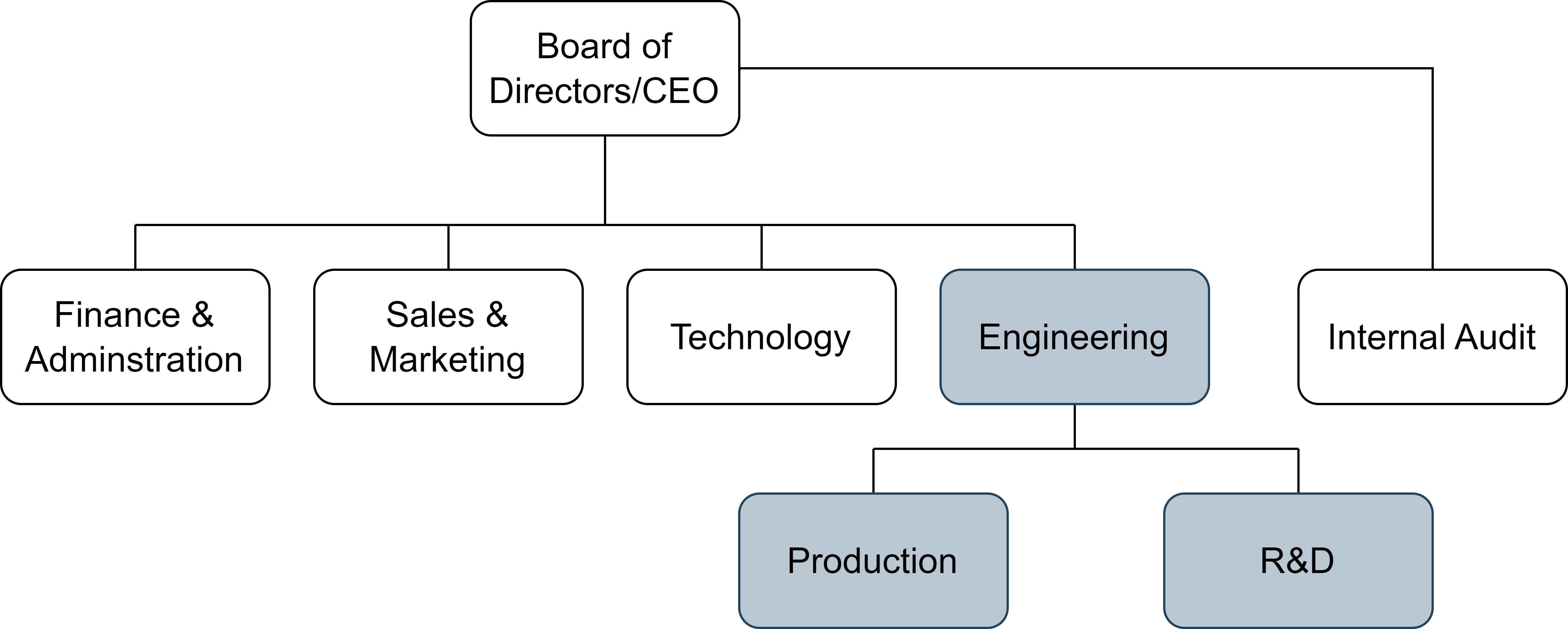
### Definition des ISMS-Anwendungsbereichs

Bei der Definition des ISMS-Anwendungsbereichs können folgende Aspekte einbezogen werden: (i) Das Personal und/oder die Mitarbeitenden, die operativ im Anwendungsbereich des ISMS tätig sind; (ii) die in den Anwendungsbereich des ISMS einbezogenen Prozesse und Dienstleistungen; (iii) die für den täglichen Geschäftsbetrieb erforderlichen Informationsbestände und -systeme; (iv) die Richtlinien, Verfahren und die erforderliche Dokumentation für den ISMS-Betrieb; (v) die Schnittstellen und Abhängigkeiten des ISMS; (vi) die IKT-Infrastruktur und der physische Standort des ISMS. Der ISMS-Anwendungsbereich sollte Folgendes widerspiegeln:

* Die von den Mitarbeitenden verwendeten Verfahren, wie Unternehmensrichtlinien, Betriebshandbücher, Sicherheitsrichtlinien und -verfahren
* Vertriebs- und Kundendienstinformationen, wie Kundendaten, Kundenaufträge, Rechnungen, interne Kundendaten und Daten anderer Unternehmen
* Geschäftsprozesse, Anwendungen und Dienstleistungen, wie Auftragsabwicklung, E-Commerce, Kundenanfragen und IT-Dienste
* Technische und nicht-technische Schnittstellen und Abhängigkeiten
* Die verwendete Technologie, wie Desktop-Computer, andere IT-Ausrüstung, Netzwerke, Telefone, Handys und Tablets
* Den physischen Standort der Vertriebs- und Serviceabteilung (z. B. Berlin)

Die Abbildung unten zeigt den ISMS-Anwendungsbereich für eine technische Abteilung in einem Unternehmen. Es handelt sich um einen Teil einer größeren Organisation. Dieses Beispiel veranschaulicht ein ISMS, das sich auf einen spezifischen Bereich des Unternehmens bezieht und nicht das gesamte Unternehmen umfasst.

Beispiel für eine Organisationsstruktur, die den ISMS-Anwendungsbereich widerspiegelt



Quelle: Andrew Sai (2023).

Es gibt drei wesentliche Schritte, um den Anwendungsbereich der ISMS-Implementierung für eine Organisation zu bestimmen:

1. Identifizierung der Räumlichkeiten, Strukturen und Standorte, an denen relevante Informationen gespeichert sind, einschließlich physischer und digitaler Dokumente.
2. Identifizierung aller möglichen Methoden, mit denen die Informationen den Nutzer:innen zugänglich gemacht werden, wie beispielsweise Berechtigungen, Netzwerksysteme und Kommunikationskanäle.
3. Festlegung der Grenzen des Anwendungsbereichs, das heißt, was innerhalb des ISMS-Anwendungsbereichs liegt und welche Bereiche möglicherweise außerhalb der Kontrolle der Organisation liegen, wie zum Beispiel ausgelagerte Produkte oder Dienstleistungen.

Es wird empfohlen, das PDCA-Modell (Plan-Do-Check-Act) als nützliches Framework für die Festlegung, Implementierung, Überwachung, Steuerung und Pflege eines ISMS zu verwenden.

PDCA-Modell und ISMS

Diagramm

Beschreibung automatisch generiert

Quelle: Andrew Sai (2023).

Früher wurde in der ISO/IEC 27001:2005 das Plan-Do-Check-Act-Modell (auch bekannt als Demings Qualitätskreis) als Grundlage für die Festlegung, Implementierung, Überwachung, Steuerung und Pflege des ISMS in einer Organisation vorgeschrieben. In der ISO/IEC 27001:2013 wurde dies aktualisiert, indem die Einführung, Umsetzung, Pflege und fortlaufende Verbesserung des ISMS in Übereinstimmung mit den Standards als Empfehlung für Organisationen festgelegt wurde und die PDCA-Anforderung gestrichen wurde. Daher wird die Anwendung des PDCA-Modells als Empfehlung angesehen.

Der PDCA-Zyklus ist ein empfohlener Ansatz, um langfristig eine fortlaufende Verbesserung des ISMS zu gewährleisten und bildet die Grundlage zahlreicher Managementsysteme. Es ist wichtig anzumerken, dass das PDCA-Modell zur fortlaufenden Anpassung des ISMS-Anwendungsbereichs dient. In unserem Beispiel der technischen Abteilung könnte es bestimmte Aspekte der ISMS-Implementierung geben, die außerhalb des Anwendungsbereichs liegen (z. B. die fälschliche Einbeziehung der Abteilungen Vertrieb und Marketing in die Implementierung), die mithilfe des PDCA-Modells identifiziert werden könnten. Sobald der Anwendungsbereich identifiziert ist, könnte er auf die technische Abteilung begrenzt werden, wo er benötigt wird.

### PDCA-Phasen

Im Folgenden werden die einzelnen Phasen des PDCA-Modells aus der vorherigen Abbildung erläutert.

#### Plan (Gestaltung des ISMS)

In der „Plan“-Phase wird die Informationssicherheitspolitik entwickelt und dokumentiert. Es werden Informationssicherheitsziele, Prozesse und Verfahren definiert. Zu den Aufgaben in dieser Phase gehören:

* Auswahl eines geeigneten Sicherheitsreifegradmodells oder Frameworks,
* Identifizierung geeigneter Beurteilungsinstrumente,
* Durchführung von Sicherheitsbeurteilungen.

#### Do (Implementierung des ISMS)

Die „Do“-Phase befasst sich mit der Implementierung der Informationssicherheitspolitiken und der entsprechenden Verfahren des ISMS. In dieser Phase werden Verantwortlichkeiten für Prozesse, Systeme und Verfahren festgelegt. Zu den Aufgaben in dieser Phase gehören:

* Implementierung von Sicherheitsmaßnahmen,
* Entwicklung von Sicherheitspolitiken,
* Schulung des Personals.

#### Check (Überwachung und Überprüfung des ISMS)

In der „Check“-Phase werden Maßnahmen durchgeführt, um sicherzustellen, dass das ISMS ordnungsgemäß implementiert wird. Dies umfasst Selbstbeurteilungen wie interne Audits und mögliche Überprüfungen durch Dritte. Zu den Aufgaben in dieser Phase gehören:

* Überprüfung der Sicherheitsmaßnahmen,
* Durchführung von Selbstbeurteilungen,
* Gegebenenfalls Überprüfung durch externe Stellen.

#### Act (Pflege und Anpassung des ISMS)

In der letzten Phase, der „Act“-Phase, werden Korrekturen an Mängeln im ISMS vorgenommen und präventive Maßnahmen basierend auf den Ergebnissen der Beurteilung des ISMS umgesetzt. Zu den Aufgaben in dieser Phase gehören:

* Lehren aus Erfahrungen ziehen,
* Festlegung von Leistungsindikatoren,
* Anpassung des ISMS nach Bedarf,
* Wiederholung des Zyklus.

Das PDCA-Modell hat sich als nützlicher Leitfaden für die Ausrichtung des ISMS-Anwendungsbereich erwiesen.

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie drei mögliche Grenzen eines ISMS.

*Aktivitäten einer Geschäftseinheit innerhalb einer Organisation*

*Aktivitäten einer Abteilung innerhalb einer Organisation*

*Projektaktivität*

*Eine Reihe von Funktionen oder Dienstleistungen*

1. Bitte markieren Sie die falsche(n) Aussage(n).

* Die Implementierung eines ISMS in einer Organisation minimiert die Auswirkungen von Sicherheitsvorfällen auf das Geschäft und die finanziellen Kosten.
* Die Implementierung eines ISMS in einer Organisation reduziert die Anzahl und Häufigkeit von Zwischenfällen.
* Die Implementierung eines ISMS in einer Organisation entspricht den Gesetzen und Vorschriften.
* *Die Implementierung eines ISMS in einer Organisation steigert den Umsatz.*

1. Bitte vervollständigen Sie den folgenden Satz.

Das Plan-Do-Check-Act-Modell (Demings Qualitätszirkel) wurde früher in der *ISO/IEC 27001:2005* gefordert, wurde jedoch in die *ISO/IEC 27001:2013* übernommen.

Zusammenfassung

Die Risiken im Zusammenhang mit IT-Systemen in Organisationen nehmen ständig zu. Sowohl Unternehmen als auch Einzelpersonen müssen ihre Herangehensweise an die Informationssicherheit anpassen, da sie insbesondere über das Internet zunehmend gefährdet sind. Für Organisationen ist es entscheidend, den ISMS-Anwendungsbereich richtig zu definieren und ihn mit den Zielen der Organisation und dem Engagement der obersten Leitung in Einklang zu bringen, um einen erfolgreichen Start zu gewährleisten.

Die Normenfamilie ISO/IEC 27000 bietet die notwendigen Leitlinien, die auf bewährten und weltweit anerkannten Praktiken basieren, um Bedrohungen und Schwachstellen zu managen und die mit IT-Systemen verbundenen Risiken zu mindern.

Grundsätzlich sollte es Organisationen jeder Größe, Art und Struktur möglich sein, ein ISMS zu implementieren. Das ISMS ist kein einheitliches Konzept, sondern eine Reihe von Richtlinien, die in bestehende Geschäftsprozesse und Abläufe integriert werden sollen. Die Anforderungen sind in Normen definiert. Die Umsetzung kann jedoch anspruchsvoll sein und erfordert erfahrene ISO-Sicherheitsexpert:innen, welche die oberste Leitung bei der Implementierung unterstützen.

Dokumentation ist ein zentrales Thema bei der Implementierung eines ISMS.

# Lektion 3 – Implementierung des Informationssicherheitsmanagementsystems

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… können Sie die erforderlichen Schritte beschreiben, um ein ISMS gemäß den Spezifikationen der Normen ISO/IEC 27001 und 27002 in einer Organisation zu implementieren.

… sind Sie in der Lage, ein Statement of Applicability (SoA) zu formulieren, in dem erklärt wird, welche Sicherheitsmaßnahmen angewendet oder ausgeschlossen werden und dies zu begründen.

… können Sie eine Organisationsstruktur definieren, einschließlich der Rollen und Verantwortlichkeiten für die Informationssicherheit.

… sind Sie in der Lage, Dokumentation und Kommunikation zu entwickeln und zu verwalten, um den relevanten ISO-Normen gerecht zu werden.

… können Sie Sicherheitsmaßnahmen bewerten und geeignete Maßnahmen und Verfahren zur effektiven Ausführung des ISMS entwickeln und implementieren.

# 3. Implementierung des Informationssicherheitsmanagementsystems

## Einführung

Die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) wird oft als Herausforderung angesehen. Dies liegt vor allem daran, dass die ISO-Normen allgemeine Leitlinien für die Implementierung bieten und die Kontextfaktoren von Organisation zu Organisation unterschiedlich sein können. Da sich Organisationen in Größe und Art unterscheiden, gibt es keine festen Regeln für die Umsetzung.

Organisationen jeder Art und Größe sind auf jeder Ebene mit bestimmten Risiken konfrontiert, die sich aus Bedrohungen und Schwachstellen ergeben. Häufig werden diese nicht adäquat adressiert und es fehlen wirksame Kontrollmechanismen. Der entscheidende Faktor zwischen einer effektiven und einer ineffizienten Organisation ist in der Regel das Risikomanagement. Organisationen, die in der Lage sind, Risiken zu bewerten, zu managen und die Auswirkungen von Risiken auf ihre Systeme und Prozesse zu minimieren, haben bessere Erfolgsaussichten.

Diese Lektion beschreibt in Übereinstimmung mit ISO/IEC 27001, wie ein ISMS implementiert wird. Dazu gehört die Festlegung der Ziele und des Anwendungsbereichs des ISMS. Die Lektion behandelt die Inventarisierung der Assets, die Definition eines Risikomanagement-Frameworks, die Identifizierung und Bewertung von Risiken sowie die Risikobehandlungspläne. Darüber hinaus werden der Auditplan auf der Grundlage der in Anhang A der ISO/IEC 27001 und 27002 aufgeführten Maßnahmen und Verfahren, das Dokumentations- und Kommunikationsmanagement sowie die Erstellung einer Erklärung zur Anwendbarkeit (SoA) behandelt. Die Definition von Rollen und Verantwortlichkeiten sowie die Dokumentation und andere Maßnahmen, die zur erfolgreichen Umsetzung des ISMS beitragen, werden ebenfalls in dieser Lektion behandelt.

## 3.1 Risikobeurteilung

Die Implementierung eines ISMS ist mit Risiken verbunden. Risiken sind eine Funktion von Bedrohungen und Schwachstellen. Mit anderen Worten: Risiken sind mathematisch gesehen gleich Bedrohungen multipliziert mit Schwachstellen. Die frühzeitige Identifizierung von Risiken ist ein positiver Schritt in die richtige Richtung. Organisationen sind jedoch ständigen Veränderungen unterworfen und diese Veränderungen können neue Risiken für das ISMS und die Organisation mit sich bringen. Mögliche Veränderungen können sich aus verschiedenen Faktoren ergeben, wie z. B.:

* Änderungen im Geschäftsumfeld, einschließlich rechtlicher, regulatorischer und anderer externer Faktoren.
* Änderungen im Risikoprofil, das durch verschiedene Variablen beeinflusst wird, einschließlich der Art und des Ausmaßes der Bedrohungen, denen eine Organisation ausgesetzt ist, sowie interne und externe Einflussfaktoren.
* Veränderungen in den Geschäftszielen, die dazu führen, dass die Organisation ihre Ziele anpasst oder neue Ziele entwickelt.
* Änderungen in der Geschäftsstrategie, welche die Gesamtausrichtung der Organisation beeinflussen.
* Betriebsbedingungen, die sich auf die täglichen Aktivitäten der Organisation auswirken.
* Marktbedingungen, wie z. B. Wettbewerb oder Veränderungen in der Branche, in der die Organisation tätig ist.
* Technologische oder infrastrukturelle Änderungen, wie z. B. Änderungen an Informationssystemen oder physischen Standorten sowie Hardware-Upgrades.

Im Risikomanagementprozess nach ISO/IEC 31000 beginnt die Risikobeurteilung (Klausel 5.4) nach der Definition des organisatorischen Kontextes (sowohl intern als auch extern) (Klausel 5.3), der Identifizierung der Risiken (Klausel 5.4.2), der Analyse der Risiken (Klausel 5.4.3), der Bewertung der Risiken (Klausel 5.4.4) und der angemessenen Behandlung der Risiken (Klausel 5.5).

Die folgende Abbildung zeigt schematisch die Schritte im Risikomanagementprozess, soweit es um die Implementierung des ISMS geht. Es ist wichtig zu wissen, dass der erste Schritt in der Kontextermittlung besteht. Ebenso wichtig ist es zu beachten, dass die Kommunikation und Konsultation (Klausel 5.2) sowie die Überwachung und Überprüfung (Klausel 5.6) der Prozesse ein notwendiger Bestandteil des gesamten Prozesses sind, wie es die **ISO/IEC 31000** (Risikomanagement) vorschreibt.

**ISO 31000**

Hierbei handelt es sich um eine Familie von Normen, die sich auf das Risikomanagement beziehen und in der International Organization for Standards (ISO) kodifiziert sind.

Risikomanagementprozess

Diagramm

Beschreibung automatisch generiert

Quelle: Andrew Sai (2023). Der Text basiert auf ISO/IEC 31000. Quelle (ISACA, 2016, basierend auf ISO/IEC 31000 Risikomanagement-Framework)

Die ISO/IEC 27001:2013 definiert **Risiko** als das Potenzial von Ereignissen und Konsequenzen, die sich negativ auf die Informationssicherheitsziele einer Organisation auswirken können. Diese Definition lässt verschiedene Interpretationen zu, wobei sich das zentrale Konzept um die Folgen oder Auswirkungen eines Ereignisses dreht. Beispielsweise kann ein gehacktes System zu einem kompromittierten System führen, das anfällig für die böswilligen Handlungen des Hackers ist.

**Risiko**

Die ISO 27001:2013 definiert Risiko als „die Auswirkung von Unsicherheit (auf Ziele)“.

Risikomanagement beinhaltet bewusste Anstrengungen, um Unsicherheiten in Bezug auf das Erreichen von Risikozielen, Ergebnissen, Zielevorgaben und Ergebnissen des ISMS zu managen. Der Risikomanagementprozess beginnt in der Regel mit einer Risikobeurteilung. Laut ISACA (2016) ist Risikomanagement „ein umfassender Prozess innerhalb eines Managementsystems. In einem ISMS soll es zur systematischen Identifizierung, Beurteilung und transparenten Darstellung von Risiken im Kontext der Informationssicherheit beitragen und eine akzeptable/langfristige Verbesserung des Sicherheitsniveaus im ISMS-Anwendungsbereich gewährleisten“ (ISACA, 2016, Seite 19).

Einige konkrete Ziele des Risikomanagements sind:

* Früherkennung und Minderung von Informationssicherheitsrisiken
* Entwicklung einer Beurteilungsmethode für identifizierte Risiken
* Zuweisung von Verantwortlichkeiten für das Management identifizierter Risiken
* Dokumentation der Risiken einschließlich ihrer Beurteilung
* Implementierung einer angemessenen Behandlung von identifizierten Risiken

Das Risikomanagement kann in den folgenden Schritten durchgeführt werden, wobei diese Liste nicht erschöpfend ist:

* Identifizierung der Risiken
* Analyse der Risiken
* Beurteilung der Risiken
* Behandlung der Risiken

Wir wollen nun jeden dieser Schritte näher betrachten und mit Schritt 1 beginnen.

### Risikoidentifikation

Bei der Risikoidentifikation geht es um die Identifizierung, Beschreibung und Auflistung potenzieller Risiken, die sich negativ auf die Geschäftsergebnisse einer Organisation auswirken können. Diese Risiken können sich auf die Leistung, Qualität, Schäden, Verluste oder den Ruf der Organisation auswirken. Risiken werden oft als ein inhärentes Ergebnis der Nutzung von IT-Systemen und -Technologien (ob neu oder alt) betrachtet. Die ISO/IEC 27001:2013 empfiehlt, Informationssicherheit als ganzheitliche Aufgabe zu betrachten und nicht auf bestimmte Aspekte der Organisation zu beschränken. Es gibt zahlreiche Quellen für Sicherheitsrisiken für die Informationswerte einer Organisation. Diese Risiken resultieren in der Regel aus Bedrohungen und Schwachstellen. Sicherheitsrisiken können zum Beispiel von folgenden Faktoren ausgehen:

* Interne und externe Quellen, insbesondere wenn Daten über Netzwerke ausgetauscht werden.
* Interne organisatorische Änderungen.
* Veraltete und nicht aktualisierte Systeme und Anwendungen.
* Zusammenarbeit mit Zulieferern und externen Organisationen.
* Zugang zu Unternehmensnetzwerken, möglicherweise über BYOD (Bring Your Own Device), unsichere Verbindungen oder Dritte.
* Naturkatastrophen, die sich auf die Systeme auswirken können (z. B. Erdbeben).
* Sabotage und kriminelle Handlungen.
* Social Engineering und Insider-Bedrohungen.

Die Identifizierung von Risiken erfolgt in der Regel durch interne und externe Audits, Auditberichte, ähnliche Untersuchungen oder Nachforschungen zu spezifischen Aspekten der Geschäftstätigkeit einer Organisation. Bei diesen Audits werden die Organisation und ihre Sicherheitsvorkehrungen überprüft und Empfehlungen für den Umgang mit den festgestellten Risiken ausgesprochen. Risiken können auch durch eine explizite Risikoanalyse ermittelt werden, die für bestimmte Projekte, Geschäftsprozesse usw. durchgeführt wird. Risiken können auch im Tagesgeschäft identifiziert werden. Beispielsweise könnte eine Schwachstelle bei der Nutzung eines CRM-Systems von Mitarbeitenden der Kundenbetreuungsabteilung erkannt und an die IT-Abteilung gemeldet werden, damit geeignete Maßnahmen ergriffen werden können. Diese Art von Risiko zeigt Schwachstellen in den IT-Systemen der gesamten Organisation auf und verdeutlicht, wie leicht Kundendaten für böswillige Zwecke missbraucht werden können, wenn sie in die falschen Hände geraten.

### Risikoanalyse

Dies ist der zweite Schritt nach der Identifizierung des Risikos bzw. der Risiken. Bei der Risikoanalyse sollten die Eintrittswahrscheinlichkeit und die möglichen Auswirkungen, wenn das Risiko eintritt, klar bestimmt und dokumentiert werden.

**Risikokriterien**

Rahmenbedingungen, anhand derer die Bedeutung eines Risikos bewertet wird (NIST).

Die Risikoanalyse basiert auf definierten und akzeptierten **Risikokriterien**, die insbesondere mit der obersten Leitung abgestimmt sind. Diese Kriterien umfassen organisatorische Ziele, interne und externe Abhängigkeiten sowie verbindliche Anforderungen wie Normen, Gesetze und Politiken.

Der Ansatz zur Risikoanalyse kann quantitativ, qualitativ oder eine Kombination aus beidem sein. Die ISO-Normen bevorzugen tendenziell einen qualitativen Ansatz, bei dem die Risikoberechnung nicht im Vordergrund steht. Stattdessen werden Methoden verwendet, die helfen, Vermögenswerte, Risikoverantwortliche, identifizierte Bedrohungen, Schwachstellen und Auswirkungen in Form eines Risikoprotokolls zu erfassen.

### Risikobewertung/-beurteilung

Die Risikobeurteilung ist ein systematischer Prozess, bei dem die Vermögenswerte, Bedrohungen, Schwachstellen und Auswirkungen einer Organisation untersucht werden, um die Wahrscheinlichkeit und die Folgen von Risiken zu bewerten. Der Beurteilungsprozess führt oft zu einer Risikokategorisierung oder -matrix und schließlich zu einer Punktzahl. Durch die Risikobeurteilung wird eine Zahl oder Punktzahl ermittelt, die den Grad des mit einem Ereignis oder einer Einrichtung verbundenen Risikos angibt.

Die Risikobeurteilung ist in Klausel 6.1.2 der ISO-Normen festgelegt und erfordert, dass die Organisation einen Prozess zur Beurteilung der Informationssicherheitsrisiken definiert und anwendet (Klausel 6 der ISO/IEC 27001:2013). Dabei muss die Methode zur Beurteilung der Risiken geeignet sein für die Organisation, ihre Sicherheitsziele und andere Anforderungen wie geschäftliche, rechtliche und regulatorische Belange. Obwohl ISO/IEC 31000 (eine Familie von Normen zum Risikomanagement) und ISO/IEC 27005 (konzentriert auf das Risikomanagement der Informationssicherheit) Leitlinien bereitstellen, gibt es dennoch Flexibilität bei der Risikobeurteilung. Die gewählte Methodik sollte dabei helfen, Risiken zu erkennen, Verantwortliche für die Risikobeurteilung zu bestimmen und Kriterien für die Risikoakzeptanz festzulegen. Außerdem muss sie in der Lage sein, Risiken in Bezug auf ihre Wahrscheinlichkeit und Auswirkungen zu analysieren. Die Beurteilung ist ein formeller Prozess, der geplant und dokumentiert werden muss.

### Risikobehandlung

Organisationen sind verpflichtet, Maßnahmen zur Risikobehandlung gemäß den Empfehlungen in Anhang A der ISO/IEC 27001 umzusetzen und ein Statement of Applicability (SoA) als Teil des ISMS-Implementierungsprozesses zu entwickeln. Anhang A enthält eine umfassende Liste von 114 Sicherheitsmaßnahmen, die in 14 Kategorien unterteilt sind. In der aktualisierten Version 2022 wurden diese Maßnahmen auf 93 reduziert und in vier Hauptbereiche unterteilt: organisatorisch, personell, physisch und technologisch.

**Risikobereitschaft**

Das Risikoniveau, das eine Organisation bei der Verfolgung ihrer Ziele zu akzeptieren bereit ist, bevor sie Maßnahmen zur Risikominderung ergreift.

Die wichtigsten Maßnahmenkategorien in Anhang A der ISO 27001:2013, die jedoch in der Ausgabe 2022 neu geordnet wurden, sind wie folgt:

1. A.5 Informationssicherheitspolitik
2. A.6 Informationssicherheitsorganisation
3. A.7 Sicherheit des Personals
4. A.8 Vermögenswertmanagement
5. A.9 Zugangskontrolle
6. A.10 Kryptografie
7. A.11 Physische und umgebungsbezogene Sicherheit
8. A.12 Betriebssicherheit
9. A.13 Sicherheit der Kommunikation
10. A.14 Beschaffung, Entwicklung und Wartung von Systemen
11. A.15 Beziehungen zu Lieferanten
12. A.16 Handhabung von Informationssicherheitsvorfällen
13. A.17 Informationssicherheitsaspekte im Business Continuity Management
14. A.18 Compliance

Das Hauptziel von Anhang A besteht darin, Organisationen bei der Auswahl und Implementierung geeigneter Maßnahmen auf der Grundlage ihrer Risikobeurteilung und -behandlung zu unterstützen. Dies ermöglicht es Organisationen, spezifische Risiken im Zusammenhang mit ihren Informationsbeständen und -prozessen anzugehen, die Einhaltung von Industriestandards, gesetzlichen und behördlichen Anforderungen nachzuweisen und ihre allgemeine Sicherheitslage zu verbessern.

Es ist wichtig zu beachten, dass Organisationen nicht verpflichtet sind, alle 114 Maßnahmen oder die reduzierte Version mit 93 Maßnahmen in Anhang A umzusetzen. Stattdessen können sie die für sie relevanten Maßnahmen auf der Grundlage ihrer Risikobeurteilung und ihrer geschäftlichen Anforderungen auswählen. Die Implementierung der relevanten Maßnahmen aus Anhang A hilft Organisationen, eine solide Sicherheitsbasis zu schaffen und Risiken effektiv zu managen.

Die SoA spielt eine zentrale Rolle als Bindeglied zwischen der Risikobeurteilung und dem Risikomanagement in einer Organisation und ist daher für den Implementierungsprozess des ISMS von entscheidender Bedeutung. Darüber hinaus sollte für jede identifizierte Risikoart und -klasse klar definiert werden, wer für das Risiko verantwortlich ist, basierend auf den festgelegten Risikokriterien.

Ein grundlegendes Prinzip für den Umgang mit Risiken ist die **Risikobereitschaft** der Organisation. Dies wird häufig in einer Risikopolitik oder einem anderen Dokument mit Managementleitlinien festgelegt, um die Organisation bei der Risikobeurteilung und dem Risikomanagement zu leiten. ISO/IEC 27005:2011 bietet einen Ausgangspunkt für ein Risikobehandlungsmodell. Einige typische Optionen für das Risikomanagement gemäß ISO/IEC 27005 sind:

* **Risikominderung**: Hier werden vorbeugende, abschreckende oder aufdeckende Kontrollmethoden eingesetzt, um das identifizierte Risiko zu reduzieren.
* **Risikovermeidung**: Dies beinhaltet Entscheidungen, sich nicht mit identifizierten oder risikobehafteten Risiken zu befassen. Aktivitäten, die zu diesen Risiken führen können, werden beendet. Mit solchen Risiken verbundene Pläne oder Projekte können verschoben oder gestrichen werden, abhängig von den Risikokriterien und der Risikobereitschaft der Organisation.
* **Risikotransfer**: Eine andere Partei, wie z. B. eine Versicherungsgesellschaft, ein Lieferant, ein externer Dienstleister oder eine andere Drittpartei, wird beauftragt, das identifizierte Risiko zu teilen. Organisationen versichern in der Regel ihre Vermögenswerte und übertragen damit das Risiko auf einen Dritten. Wenn Sie beispielsweise als Privatperson ein Auto kaufen und besitzen, sind Sie dafür verantwortlich. Der Abschluss einer Versicherung und die Zahlung von Versicherungsprämien an eine Versicherungsgesellschaft entlasten Sie jedoch im Falle eines Unfalls, je nach gewählter Versicherungsvariante.
* **Risikoakzeptanz**: Es geht darum, erkannte oder potenzielle Risiken als Chancen zu begreifen, die es zu nutzen gilt. Das bedeutet, dass es im Rahmen der Strategie, der Ziele oder der Risikobereitschaft der Organisation oft keine andere Möglichkeit gibt, mit diesen Risiken umzugehen. Die von den Organisationen akzeptierten Risiken sind oft gering und liegen innerhalb der Möglichkeiten des Managements der Organisation.

Die Optionen für das Risikomanagement basieren auf den Ergebnissen der Risikobeurteilung. Die folgende Abbildung zeigt eine beispielhafte Risikomatrix zur Beurteilung der Auswirkungen und der Wahrscheinlichkeit eines Risikos. Eine Risikomatrix (oder Kategorisierung) hilft der Organisation zu unterscheiden, welche Risiken priorisiert werden sollten und welche Behandlungsoptionen zur Verfügung stehen.

Beispiel einer Risikomatrix in MS Excel

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Auswirkungen** | | | | |
| **Unbedeutend** | **Gering** | **Mäßig** | **Schwerwiegend** | **Extrem** |
| **Wahrscheinlichkeiten** | **Beinahe sicher** | Mittel | Hoch | Sehr hoch | Sehr hoch | Sehr hoch |
| **Wahrscheinlich** | Mittel | Hoch | Hoch | Sehr hoch | Sehr hoch |
| **Möglich** | Niedrig | Mittel | Hoch | Hoch | Sehr hoch |
| **Unwahrscheinlich** | Niedrig | Niedrig | Mittel | Mittel | Hoch |
| **Selten** | Niedrig | Niedrig | Niedrig | Niedrig | Mittel |

Quelle: Andrew Sai (2023).

Zusammenfassend kann gesagt werden, dass die Optionen zur Risikobehandlung die Maßnahmen umfassen, die gemäß der Risikomatrix zur Bewältigung der identifizierten Risiken ergriffen werden. Die oben dargestellte Risikomatrix dient als Instrument zur Bewertung der Wahrscheinlichkeit und der Auswirkungen potenzieller Risiken, um Prioritäten zu setzen und fundierte Entscheidungen über das Risikomanagement zu treffen. Typische Optionen für den Umgang mit Risiken sind die Vermeidung von Risiken mit hohen Auswirkungen und hoher Wahrscheinlichkeit, die Verringerung oder Übertragung von Risiken auf eine andere Partei und die Akzeptanz von Risiken mit geringen Auswirkungen und geringer Wahrscheinlichkeit ohne besondere Maßnahmen. Selbst wenn ein Gebäude umfassend physisch und logisch gesichert ist, können Restrisiken verbleiben, z. B. das Risiko böswilliger Handlungen durch interne Mitarbeitende. Obwohl diese Risiken unwahrscheinlich sind, können sie ohne besondere Maßnahmen akzeptiert und im Management festgehalten werden. Ein weiteres Beispiel für den Umgang mit solchen Risiken könnte die Durchführung von Schulungs- und Sensibilisierungsprogrammen für Mitarbeitende sein, um das Eintreten solcher Risiken zu verhindern, während sie im Rahmen der Risikobereitschaft der Organisation akzeptiert werden.

### Fragen zur Selbstkontrolle

1. Bitte führen Sie alle Schritte des Risikomanagementprozesses auf

*Schritt 1: Identifizierung der Risiken.*

*Schritt 2: Analyse der Risiken.*

*Schritt 3: Beurteilung der Risiken.*

*Schritt 4: Behandlung der Risiken.*

1. Bitte vervollständigen Sie den folgenden Satz.

Die *STRIDE-* und die *Delphi-Methode* sind zwei der Methoden und Techniken, die als Hilfsmittel bei der Risikoidentifizierung eingesetzt werden können.

## 3.2 Erklärung zur Anwendbarkeit (SoA)

Eine **Erklärung zur Anwendbarkeit (Statement of Applicability – SoA** ) ist eine entscheidende Komponente bei der Implementierung eines ISMS, da sie als Bindeglied zwischen der Risikobeurteilung und der Risikobehandlung innerhalb einer Organisation dient. Der Umgang mit der SoA wird in Klausel 6.1.3 der ISO/IEC 27001:2013 behandelt und enthält eine Checkliste, die als Leitfaden für die Implementierung des ISMS dient. Dies wird auch in der aktualisierten Version aus dem Jahr 2022 behandelt. Diese Checkliste hilft bei der Identifizierung aller relevanten regulatorischen, rechtlichen und vertraglichen Anforderungen sowie der erforderlichen Maßnahmen, um sicherzustellen, dass die geschäftlichen Anforderungen der Organisation erfüllt werden. Die SoA ist ein wichtiges Dokument für Organisationen, die eine Zertifizierung nach ISO/IEC 27001 anstreben. Es ist zu beachten, dass die SoA nicht verpflichtend ist, jedoch dringend empfohlen wird. Der Zweck der SoA besteht darin, zu bestimmen, welche der Maßnahmen aus Anhang A des Standards auf die Informationssicherheitsrisiken der Organisation anwendbar sind, und die Umsetzung dieser Maßnahmen zu erklären.

**Erklärung zur Anwendbarkeit (SoA)**

Dies ist ein Dokument, das aus der vollständigen Liste der bewertbaren Informationssicherheitsmaßnahmen besteht, die in Anhang A von ISO 27001 angegeben und in ISO 27002 detailliert beschrieben sind.

Die ISO/IEC 27001:2013 enthält ein dokumentiertes ISMS, das 35 Maßnahmenziele mit jeweils einer oder mehreren zugehörigen Maßnahmen sowie 114 umfassende Maßnahmen zur Umsetzung des ISMS enthält. Die Maßnahmen decken verschiedene Bereiche der Informationssicherheit ab, wie Zugriffskontrolle, Asset Management, Kryptografie, Incident Management und physische Sicherheit. Die SoA sollte jede der anwendbaren Maßnahmen aus Anhang A zusammen mit einer kurzen Beschreibung zur Umsetzung jeder Maßnahme auflisten. Wenn Maßnahmen von der Umsetzung ausgeschlossen werden sollen, muss die Organisation dies begründen. Die SoA dokumentiert die Gründe für den Ausschluss bestimmter Maßnahmen sowie den Umsetzungsstatus der umgesetzten Maßnahmen. Es ist wichtig zu beachten, dass nicht alle Organisationen alle Maßnahmen umsetzen müssen, da einige für ihre spezifischen Bedürfnisse nicht relevant sind.

Die Entwicklung einer SoA erfordert ein hohes Maß an Koordination, Zeit und Mühe, wobei das Engagement und die Beteiligung des Managements entscheidend für den Erfolg sind. Auch wenn es verschiedene Ansätze für die Entwicklung einer SoA gibt, wird der folgende Prozess für die Implementierung eines ISMS empfohlen:

1. Dokumentation der durchzuführenden Aktivitäten nach einer festgelegten Methode.
2. Jeder Prozess sollte von geeigneten Maßnahmen begleitet werden, wie z. B. Audits und einer angemessenen Überprüfung oder Bewertung.
3. Festlegung eines Sicherheitsziels auf organisatorischer Ebene, das klar formuliert und den Beteiligten zugänglich gemacht wird.
4. Kontinuierliche Verbesserung aller Prozesse und Maßnahmen.

Die SoA ist wie ein Verzeichnis von Sicherheitsmaßnahmen, die auf eine bestimmte Organisation anwendbar sind. Die Auswahl der am besten geeigneten Sicherheitsmaßnahmen erfolgt nach einer gründlichen Risikoanalyse, -bewertung und -bewältigung. Die Entwicklung einer SoA kann in fünf Schritten dargestellt werden:

1. Risiken müssen identifiziert und analysiert werden.
2. Auf der Grundlage der früheren Bewertung und der den Risiken zugeordneten Behandlungsoptionen werden Sicherheitsmaßnahmen zur Risikobehandlung ausgewählt.
3. Es wird eine Risikobehandlungsplanung durchgeführt.
4. Anschließend werden Sicherheitsmaßnahmen implementiert.
5. Die SoA wird dann gepflegt.

Die Dokumentation ist ein wichtiger Aspekt der Pflege der SoA. Tabelle… unten zeigt ein Beispiel für eine Anwendbarkeitserklärungstabelle. In der Tabelle werden die relevanten Maßnahmen, welche die Prozesse und Aktivitäten begleiten, umrissen und beschrieben. Zudem wird angegeben, ob diese angewandt wurden und wie die Anwendung begründet wurde oder nicht.

Beispiel Anwendbarkeitserklärungstabelle

|  |  |  |  |
| --- | --- | --- | --- |
| Maßnahme | | Angewandt  (J/N) | Rechtfertigung |
| Referenz | **Beschreibung** |
| A.5.1.0 | Informationssicherheitspolitiken | J | ISO/IEC 27001-Anforderung |

Quelle: Andrew Sai (2023)

### Fragen zur Selbstkontrolle

1. Bitte markieren Sie die falsche(n) Aussage(n).

* Eine SoA enthält eine Checkliste, die als Orientierungshilfe für die Implementierung des ISMS dient.
* Eine SoA hilft dabei, alle relevanten regulatorischen und rechtlichen Anforderungen zu identifizieren.
* Die Entwicklung einer SoA erfordert eine Menge Koordination, Zeit und Mühe.
* *Es besteht keine Notwendigkeit, Maßnahmen auszuschließen, die nicht in einer SoA implementiert sind.*

## 3.3 Definition der Organisationsstruktur für Informationssicherheit

Es ist sinnvoll und praktikabel, in den frühen Phasen der ISMS-Implementierung eine klare Zusammensetzung und Struktur des Informationssicherheitsmanagements zu entwickeln. Eine gut durchdachte Organisationsstruktur erleichtert eine effektive Risikobeurteilung. Je nach Größe der Organisation sollten Rollen und Verantwortlichkeiten klar definiert werden, sodass das Informationssicherheitssystem und die Maßnahmen effektiv funktionieren. Es wird empfohlen, die Aktivitäten zur Informationssicherheit durch ein funktionsübergreifendes Managementforum zu koordinieren, das sich aus Vertreter:innen verschiedener Bereiche der Organisation zusammensetzt. Für die Umsetzung des ISMS wird die Bildung eines Projektteams erwartet, das von einem Mitglied der Geschäftsleitung geleitet wird und die Umsetzung des ISMS überwacht.

**Governance-Strukturen für die Informationssicherheit**

Wie jede andere Kontrollmaßnahme auf Unternehmens- oder Organisationsebene beginnt auch das ISMS mit der Governance. Der Zweck der Informationssicherheits-Governance ist es, sicherzustellen, dass alle Stellen und Akteure proaktiv angemessene Informationssicherheitsmaßnahmen durchführen, um die organisatorischen Ziele zu erreichen. Im Rahmen der Governance werden auch die wesentlichen Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit festgelegt und die Organisationsstruktur definiert, die für die Implementierung und das kontinuierliche Management des ISMS erforderlich ist.

Nach Bowen et al. (2006, S. 2) wird Informationssicherheits-Governance definiert als:

„*…der Prozess, einen Rahmen und unterstützende Managementstrukturen und -prozesse zu schaffen und aufrechtzuerhalten, um sicherzustellen, dass Informationssicherheitsstrategien mit den Geschäftszielen übereinstimmen und diese unterstützen, dass interne Richtlinien und Maßnahmen mit den geltenden Gesetzen und Vorschriften übereinstimmen und dass klare Verantwortlichkeiten festgelegt sind, alles mit dem Ziel, Risiken zu managen.*“ (Übers. d. Autors)

In der Regel fungiert die Aufsichtsbehörde der Branche oder des Sektors, in dem die Organisation tätig ist, als erste Verteidigungslinie in Bezug auf die Governance der Organisation. Unternehmen oder Organisationen unterliegen gesetzlichen und regulatorischen Anforderungen, die von diesen Aufsichtsbehörden festgelegt werden. Der nächste Schritt in der Governance-Abfolge ist die externe Prüfung. Intern gibt es den Vorstand oder das Board of Directors und einen Prüfungsausschuss. Die interne Revision fungiert als dritte Verteidigungslinie und berichtet direkt. Die zweite Verteidigungslinie umfasst Bereiche wie Finanzkontrolle, Sicherheit, Risikomanagement, Compliance und Qualitätskontrolle. Diese Abteilungen der zweiten Verteidigungslinie überwachen die Aktivitäten der ersten Verteidigungslinie, d. h. die Managementkontrollen und die internen Kontrollmaßnahmen.

Eine Organisationsstruktur für Informationssicherheit könnte in der folgenden hierarchischen Form beschrieben werden, beginnend mit der obersten Führungsebene und endend mit spezifischen Teams, die für die Durchführung von Aufgaben verantwortlich sind. Einige wichtige Positionen werden im Folgenden kurz beschrieben. Die Rollen werden als Teil der Sicherheitspositionen empfohlen, um die Informationssicherheit in der Organisation zu überwachen und zu verwalten. Es ist wichtig zu beachten, dass diese Funktionen je nach Größe der Organisation, ihren Zielen und anderen Faktoren, die als notwendig erachtet werden, vollständig oder gar nicht umgesetzt werden können.

* **Vorstand/Geschäftsführung**: Dies ist die oberste Führungsebene, welche für die Festlegung der Strategie und der Richtlinien für die Informationssicherheit der Organisation verantwortlich ist. Der Vorstand hat die oberste Entscheidungsgewalt in Fragen der Informationssicherheit und stellt sicher, dass die Organisation die einschlägigen Gesetze, Vorschriften und Standards einhält.
* **Chief Information Officer (CIO)/Chief Information Security Officer (CISO):** Der CIO oder CISO spielt eine entscheidende Rolle bei der Festlegung und Verwaltung von Richtlinien, Verfahren und Standards für die Informationssicherheit im Einklang mit den Vorgaben der Unternehmensleitung. Der CIO oder CISO ist dafür verantwortlich, die Sicherheitsvision und -strategie zu definieren, Risiken zu managen und sicherzustellen, dass Sicherheitsrichtlinien effektiv umgesetzt und aufrechterhalten werden.
* **Sicherheitslenkungsausschuss:** In einigen Organisationen ist ein funktionsübergreifendes Team mit Vertreter:innen aus verschiedenen Abteilungen wie IT, Recht, Personal und Betrieb für die Leitung, Unterstützung und Überwachung des Informationssicherheitsprogramms der Organisation zuständig. Die Aufgabe des Lenkungsausschusses besteht darin, sicherzustellen, dass die Initiativen zur Informationssicherheit mit der Gesamtstrategie und den Zielen der Organisation übereinstimmen.
* **Information Security Manager (ISM):** Ein ISM kann in verschiedenen Organisationen unterschiedliche Bezeichnungen haben, aber er beaufsichtigt den täglichen Betrieb und das Management von Informationssicherheitsprogrammen. Das ISM ist verantwortlich für die Umsetzung und Durchsetzung der Sicherheitsrichtlinien, das Risikomanagement und die Gewährleistung, dass die Sicherheitsmaßnahmen und -prozesse gut funktionieren.
* **Informationssicherheitsteams:** Je nach Größe und Komplexität der Organisation können mehrere Teams oder Einheiten für spezifische Informationssicherheitsaufgaben zuständig sein. Nachfolgend sind einige der verbreitetsten Sicherheitsteams aufgeführt:
  + **Risk Assessment and Compliance Team:** Dieses Team ist für die Identifizierung, Beurteilung und das Management von Informationssicherheitsrisiken sowie für die Einhaltung relevanter Gesetze, Vorschriften und Standards verantwortlich.
  + **Security Operations Center (SOC) Team:** Das Team überwacht, erkennt und reagiert auf Sicherheitsvorfälle und Bedrohungen. Es verwaltet auch die Sicherheitsinfrastruktur der Organisation, einschließlich Firewalls, Intrusion-Detection-and-Prevention-Systemen.
  + **Incident Response Team:** Dieses Team ist für das Management und die Reaktion auf Sicherheitsvorfälle sowie für die Untersuchung und Umsetzung von Abhilfemaßnahmen zuständig.
  + **Security Awareness and Training Team:** Dieses Team entwickelt und führt Sicherheitsschulungen und Sensibilisierungsprogramme durch, um die Mitarbeitenden über bewährte Sicherheitsverfahren und -politiken zu informieren.
  + **Informationssicherheitsprüfer:innen:** Das Team der Informationssicherheitsprüfer:innen ist für die Durchführung regelmäßiger Sicherheitsprüfungen, die Bewertung und das Testen von Sicherheitsmaßnahmen verantwortlich, damit diese effektiv sind und den relevanten Standards entsprechen.

Es ist wichtig, eine effektive Organisationsstruktur für die Informationssicherheit zu haben, die klare Kommunikations-, Verantwortungs- und Rechenschaftslinien von der obersten Führungsebene bis zu den einzelnen Mitarbeitenden umfasst. Die spezifischen Positionen und Aufgaben können je nach Struktur und Konfiguration der Organisation variieren. Die Struktur gewährleistet, dass die Informationssicherheit in die Gesamtstrategie und -kultur integriert ist.

### Fragen zur Selbstkontrolle

1. Bitte markieren Sie die falsche(n) Aussage(n).

* Der Zweck der Informationssicherheits-Governance ist es, sicherzustellen, dass alle Stellen und Akteure proaktiv angemessene Informationssicherheitsmaßnahmen durchführen, um die organisatorischen Ziele zu erreichen.
* Im Rahmen der Governance werden auch die wesentlichen Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit festgelegt und die Organisationsstruktur definiert, die für die Implementierung und das kontinuierliche Management des ISMS erforderlich ist.
* Wie jede andere Kontrollmaßnahme auf Unternehmens- oder Organisationsebene beginnt auch das ISMS mit der Governance.
* *Die Größe des Unternehmens ist für die Bestimmung der Rollen und Verantwortlichkeiten nicht relevant, damit das Informationssicherheitssystem und die Maßnahmen effektiv funktionieren.*

## 3.4 Dokumentenmanagement und Kommunikationsplan

Dokumentation und Kommunikation sind wichtige Anforderungen im ISMS-Implementierungsprozess.

### Dokumentation

Dokumente müssen erstellt, aktualisiert und bei Bedarf veröffentlicht werden. Die Dokumente müssen beschriftet und entsprechend klassifiziert werden. Die Klassifizierung hängt natürlich vom Inhalt des Dokuments ab.

Die Anzahl oder Art der Dokumente kann variieren. Auch in Bezug auf die Dokumentation und die Aufzeichnungen gibt es Flexibilität gemäß ISO/IEC 27001:2013.

Die Dokumentationsanforderungen gemäß ISO/IEC 27001:2013 (Klauseln 4-10) lauten wie folgt.

Dokumentationsanforderungen gemäß ISO/IEC 27001:2013

|  |  |
| --- | --- |
| **Dokumentationsanforderungen** | **Einschlägige Klausel der ISO/IEC 27001** |
| ISMS-Anwendungsbereich | Klausel 4.3 |
| Informationssicherheitspolitik | Klausel 5.2e |
| Beschreibung des Risikobeurteilungsprozesses | Klausel 6.1.2 |
| Beschreibung des Risikobehandlungsprozesses | Klausel 6.1.3 |
| Erklärung zur Anwendbarkeit | Klausel 6.1.3d |
| Plan zur Behandlung von Informationssicherheitsrisiken | Klausel 6.1.3e |
| Ziele der Informationssicherheit | Klausel 6.2 |
| Nachweis der Kompetenz | Klausel 7.2d |
| Nachweis der ordnungsgemäßen Ausführung der ISMS-Prozesse | Klausel 8.1 |
| Ergebnisse der Risikobeurteilung der Informationssicherheit | Klausel 8.2 |
| Ergebnisse der Behandlung von Informationssicherheitsrisiken | Klausel 8.3 |
| Nachweis der Ergebnisse der Überwachung und Messung des ISMS | Klausel 9.1 |
| Nachweis der Audit-Programme und Audit-Ergebnisse | Klausel 9.2 |
| Nachweis der Ergebnisse der Managementbewertungen | Klausel 9.3 |
| Nachweis der Art der Nichtkonformitäten und die daraufhin ergriffenen Maßnahmen | Klausel 10.1f |
| Nachweis der Ergebnisse von Korrekturmaßnahmen | Klausel 10.1g |

Andrew Sai (2023). Textquelle: basierend auf ISO/IEC 27001 (Klauseln 4-10)

Es liegt in der Verantwortung der jeweiligen Organisation, die das ISMS einführt, zu bestimmen, welche Dokumentation und Aufzeichnungen sie zusätzlich zu den von den Normen geforderten für notwendig erachtet (Klausel 8.1). Auch dies hängt von der Art, der Größe und den Bedürfnissen der jeweiligen Organisation ab.

### Kommunikation

Kommunikation ist der Schlüssel zur Operationalisierung des ISMS. Dazu gehört der Austausch mit internen und externen Stakeholdern. Die Stakeholder reichen von Mitarbeitenden und dem Vorstand bis hin zu Drittanbietern, Kund:innen und anderen. Zu diesem Zweck empfiehlt Klausel 7.4 festzulegen, welche Informationen übermittelt werden sollen, wer die Empfänger:innen sind (Klausel 7.4c) und wer die Übermittlung vornehmen soll (Klausel 7.4d). Wann die Informationen zu übermitteln sind (Klausel 7.4b) und welche Kanäle und Prozesse zu verwenden sind (Klausel 7.4e). Die folgende Abbildung zeigt, wie Sie den Kommunikationsplan entwickeln.

Entwicklung eines Kommunikationsplans

Quelle: Andrew Sai (2023), basierend auf ISACA (2017).

Im Rahmen des Kommunikationsplans sollten die Kommunikationsziele definiert werden, gefolgt von einer Analyse der Zielgruppe und der Bestimmung geeigneter Medien. Als Nächstes müssen Sie die wichtigsten Kommunikationsbotschaften identifizieren, Rollen und Aufgaben zuweisen und anschließend den Kommunikationsplan entwickeln. Das Ergebnis sollte ein detaillierter Kommunikationsplan sein. Der Kommunikationsplan ermöglicht die effektive Weitergabe von Informationen an alle Stakeholder. Die folgende Abbildung zeigt ein Beispiel für einen Kommunikationsplan, auch Kommunikationsmatrix genannt.

Kommunikationsmatrix: Interne Kommunikation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Grund für die Kommunikation | Initiator | Empfänger | Häufigkeit | Medium |
| Managementbewertung | Chief Information Security Officer (CISO) | Oberste Leitung | Jährlich | Managementbericht nach Vorlage per E-Mail + Präsentation |
| Berichterstattung | CISO | Oberste Leitung | Vierteljährlich | KPI-Bericht gemäß Vorlage per E-Mail + Präsentation |
| Sensibilisierungsschulung | CISO | Alle Mitarbeitenden innerhalb des Anwendungsbereichs | Jährlich | Schulung (Präsenzunterricht oder online) |
| IS-Newsletter | CISO | Alle Mitarbeitenden innerhalb des Anwendungsbereichs | Vierteljährlich und von Fall zu Fall, wenn eine akute Bedrohung auftritt | E-Mail |
| Risikomanagement | CISO | Oberste Leitung | Vierteljährlich, von Fall zu Fall bei akuter Bedrohung, auf Projektbasis | Balanced-Scorecard-Bericht, bei Bedarf per E-Mail |
| Sicherheitsvorfall | Support | CISO (möglicherweise andere, in Übereinstimmung mit dem SIRP) | Von Fall zu Fall | Eskalation in Übereinstimmung mit dem SIRP (Security Incident Response Process) |
| Sicherheitsvorfall | CISO | Oberste Leitung | Von Fall zu Fall | E-Mail, möglicherweise mündlich |
| Sicherheitsvorfall mit personenbezogenen Daten | CISO | Datenschutzbeauftragter | Von Fall zu Fall | E-Mail, möglicherweise auch per Telefon oder mündlich |
| Compliance-bezogener Sicherheitsvorfall | CISO | Rechtsberatungsabteilung | Von Fall zu Fall | E-Mail, möglicherweise auch per Telefon oder mündlich |

Quelle: Andrew Sai (2023). Textquelle: ISACA (2017) Seite 28.

Nachstehend finden Sie ein Beispiel für eine externe Kommunikationsmatrix.

Kommunikationsmatrix: Externe Kommunikation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Grund für die Kommunikation | Initiator | Empfänger | Häufigkeit | Medium |
| Bericht des operativen Dienstleisters | Operativer Dienstleister | CISO | Vierteljährlich | SLA-Bericht gemäß Vorlage per E-Mail |
| Extern in Auftrag gegebene CERT-/Schwachstellenanalyse | CERT | CISO/Leiter:in der IT | Wöchentlich, von Fall zu Fall | Bericht in Übereinstimmung mit dem Vertrag per E-Mail |
| Sicherheitsvorfall | CISO, möglicherweise oberste Leitung | Alle betroffenen Kund:innen/Partner | Von Fall zu Fall | in Übereinstimmung mit dem SIRP, auf der Website, per Post, per E-Mail, per Telefon |
| Sicherheitsvorfall mit kriminellem Hintergrund | CISO | Strafverfolgungsbehörden | Von Fall zu Fall | in Übereinstimmung mit dem SIRP |

Quelle: Andrew Sai (2023). Textquelle: ISACA (2017) Seite 28.

Die Kommunikationsmatrix legt die Parameter für die interne und externe Kommunikation fest, einschließlich des Zwecks, des Empfängers, der Häufigkeit und der für die Kommunikation verwendeten Medien. Es ist jedoch wichtig zu beachten, dass die ISO/IEC 27001:2013 keine spezifischen Dokumentationsanforderungen für die ISMS-Kommunikation enthält. Es liegt in der Verantwortung der Organisation, ihren Kommunikationsansatz festzulegen, sodass der Plan ihre Bedürfnisse genau widerspiegelt.

### Fragen zur Selbstkontrolle

1. Bitte markieren Sie die **richtige(n)** Aussage(n).

* Die Dokumentationsanforderungen sind in den Klauseln 1-5 der ISO/IEC 27001:2013 aufgeführt.
* Die Anforderungen an die Dokumentation sind in den Klauseln 1-3 der ISO/IEC 27001:2013 aufgeführt.
* Die Dokumentationsanforderungen sind in den Klauseln 1-11 der ISO/IEC 27001:2013 aufgeführt.
* *Die Dokumentationsanforderungen sind in den Klauseln 4-10 der ISO/IEC 27001:2013 aufgeführt.*

1. ISO/IEC 27001:2013 (Klausel 7.4) empfiehlt festzulegen, welche Informationen zu übermitteln sind, wer die Empfänger sind (Klausel 7.4c) und wer die Übermittlung durchführt (Klausel 7.4d).

## 3.5 Definition von Maßnahmen und Verfahren

Im Kontext von ISO/IEC 27001 werden Maßnahmen als Richtlinien, Leitlinien und Techniken definiert, die im Rahmen des ISMS einer Organisation umgesetzt werden, um potenzielle Risiken zu managen und zu mindern. Ihr Ziel ist es, Informationswerte vor unbefugtem Zugriff, versehentlicher oder absichtlicher Beschädigung oder anderen Bedrohungen zu schützen, die sensible Daten gefährden könnten.

Maßnahmen können im Allgemeinen in drei Haupttypen unterteilt werden:

1. **Präventive Maßnahmen:** Diese Maßnahmen zielen darauf ab, potenzielle Sicherheitsvorfälle und -verletzungen zu verhindern, bevor sie auftreten. Beispiele hierfür sind der Einsatz von Firewalls, Verschlüsselungstechnologien und Schulungsprogrammen für das Personal.
2. **Detektive Maßnahmen:** Diese Maßnahmen konzentrieren sich auf die Erkennung und Überwachung von Sicherheitsvorfällen oder laufenden Verstößen. Sie umfassen den Einsatz von Intrusion-Detection-Systemen, die Überprüfung und die Analyse von Protokollen sowie regelmäßige Sicherheitsaudits.
3. **Korrektive Maßnahmen:** Diese Maßnahmen sind eine Reaktion auf Sicherheitsvorfälle oder Verletzungen. Ihr Ziel ist es, den Schaden zu minimieren, sich von der Verletzung zu erholen und die Wiederholung solcher Ereignisse zu verhindern. Beispiele für Korrekturmaßnahmen sind Backup- und Wiederherstellungssysteme, Notfallpläne und forensische Analysen nach einem Vorfall.

Verfahren sind detaillierte Schritt-für-Schritt-Anweisungen, die festlegen, wie Aktivitäten im Zusammenhang mit Korrekturmaßnahmen durchzuführen sind. Sie sorgen für Klarheit und Konsistenz, indem sie festlegen, wer, was, wann, wo und wie die Aktivitäten durchzuführen hat. Verfahren können Aufgaben wie die regelmäßige Aktualisierung der Systemsoftware, die Durchführung von Risikobeurteilungen, die Verwaltung von Zugriffsrechten, den Umgang mit Sicherheitsvorfällen und den sicheren Umgang mit sensiblen Daten dokumentieren. Durch Verfahren stellen Organisationen sicher, dass die für die Pflege des ISMS verantwortlichen Mitarbeitenden über die erforderliche Kompetenz verfügen und die notwendigen Maßnahmen sorgfältig durchführen, um die Wirksamkeit des ISMS zu gewährleisten.

Maßnahmen und Verfahren sind wesentliche Elemente, die im Rahmen von ISO/IEC 27001 umgesetzt werden und das Rückgrat des ISMS in der Organisation bilden. Sie bieten einen Rahmen für das effektive Management von Informationssicherheitsrisiken.

Nach der Auswahl der Risikobehandlungsoptionen müssen eine Reihe von Maßnahmen umgesetzt werden. Diese sind in Anhang A der ISO/IEC 27001:2013 beschrieben. Es ist wichtig, bestehende Maßnahmen zu evaluieren, sodass geplante neue Maßnahmen nicht mit bestehenden Maßnahmen in Konflikt geraten und nahtlos ineinander greifen. Maßnahmen können in Form von Richtlinien, Verfahren, Plänen oder Techniken vorliegen und bilden ein Maßnahmen-Framework. Es ist zu beachten, dass diese Maßnahmen und Verfahren managementorientiert und nicht notwendigerweise IT-bezogen sind. Das Maßnahmensystem ist gemäß ISO/IEC 27001 wie folgt strukturiert.

Beispiele für Richtlinien und Verfahrensmaßnahmen sind die Informationssicherheitspolitik und -verfahren, Richtlinien zur akzeptablen Nutzung, Zugriffskontrollpolitiken und -verfahren, Datensicherungsverfahren, sichere Betriebsverfahren, Systemwechsel, Einstellungsverfahren und die Handhabung von Informationssicherheitsvorfällen. Es gibt auch Prozessmaßnahmen wie Rollenzuweisung, Verantwortlichkeiten, Risikobeurteilungs- und -behandlungsverfahren usw.

Die Politiken bilden weiterhin die Grundlage für diese Maßnahmen und Verfahren. Informationssicherheitspolitiken sind hochrangige Politiken der obersten Leitung. Klausel 5.2 der ISO/IEC 27001 definiert eine Informationssicherheitspolitik für die oberste Leitung, die als übergeordnete Richtlinie und Leitbild einer Organisation dient. Dieses Grundsatzdokument enthält Ziele für die Informationssicherheit, eine Verpflichtung zur Erfüllung dieser Anforderungen (Klausel 4.1 und 4.2) und zur fortlaufenden Verbesserung des ISMS (wie in Klausel 10 der Norm gefordert). Die Informationssicherheitspolitik sollte folgende Aufgaben erfüllen:

* Definition des Umfangs, der Bedeutung und der Ziele der Informationssicherheit.
* Mitarbeitende und Stakeholder auf ihre Pflichten und Verantwortlichkeiten aufmerksam machen.
* Information über akzeptable und inakzeptable Verhaltensweisen und die Nutzung der Ressourcen der Organisation.
* Klarstellung der Verpflichtung zur Einhaltung von Gesetzen und Vorschriften.
* Verweis auf andere Grundsatzdokumente, die das Personal kennen und befolgen sollte.

### Fragen zur Selbstkontrolle

1. Bitte markieren Sie die falsche(n) Aussage(n).

* Nach der Auswahl der Optionen für das Risikomanagement ist eine Reihe von Maßnahmen durchzuführen.
* Die Maßnahmen sind in Anhang A der ISO/IEC 27001:2013 beschrieben.
* Vorhandene Maßnahmen sollten beurteilt werden.
* *Maßnahmen werden ausschließlich in Form von Richtlinien, Verfahren, Plänen oder Techniken durchgeführt.*

1. Bitte vervollständigen Sie den folgenden Satz.

Beispiele für Richtlinien und Verfahrensmaßnahmen sind die *Informationssicherheitspolitik und -verfahren*, *Richtlinien zur akzeptablen Nutzung*, *Zugriffskontrollpolitiken und -verfahren.*

Zusammenfassung

Die Grenzen der Informationssicherheit haben sich in den letzten Jahren verschoben und werden sich weiter verschieben. Traditionelle Sicherheitsmaßnahmen wie Patch-Management und Firewalls reichen nicht mehr aus, da sich Technologie, Fortschritt und Vernetzung ständig weiterentwickeln. Die Veränderungen im Anwendungsbereich und Fokus der Informationssicherheit erfordern eine stärkere Betonung des Risikomanagements.

Risikomanagement ist ein zentraler Bestandteil der Implementierung eines ISMS. Um die Informationssicherheit in einer Organisation effektiv zu gewährleisten, ist es wichtig, eine geeignete Struktur zu schaffen und die Rolle der Sicherheit auf Vorstandsebene zu stärken. Die Leitungsebene sollte die Umsetzung von Informationssicherheitsprojekten, einschließlich des ISMS, koordinieren und sicherstellen, dass die entsprechenden Dokumente gepflegt werden, um eine einfache Bezugnahme und Nachverfolgung zu ermöglichen. Bei der Bildung von Sicherheitsgruppen sollten funktionsübergreifende Teams bevorzugt werden.

Diese Lektion konzentrierte sich auf den Risikomanagementprozess, von der Risikoidentifizierung bis zur Behandlung und den erforderlichen Maßnahmen. Es wurde erläutert, warum die Erstellung einer SoA für die Implementierung eines ISMS von entscheidender Bedeutung ist, wann und warum sie erstellt werden sollte und welche Informationen sie enthalten sollte. Die sich ständig ändernden Rollen und Verantwortlichkeiten in der sich entwickelnden Informationssicherheitslandschaft wurden im Kontext der Sicherheitsorganisationsstruktur behandelt. Darüber hinaus wurden die Dokumentation, einschließlich der SoA, und die Entwicklung eines Kommunikations-Frameworks für die Kommunikation mit internen und externen Stakeholdern diskutiert. Abschließend wurde eine Definition der Maßnahmen und Verfahren gegeben, wie sie im Anhang A der ISO/IEC 27001 festgelegt sind.

# Lektion 4 – Kontrolle des Informationssicherheitsmanagementsystems

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… kennen Sie die Anforderungen an die Überwachung, Bewertung und Messung des ISMS als Teil der Kontrolle des Implementierungsprozesses und können diese diskutieren.

… sind Sie in der Lage, den gesamten ISMS-Überwachungsprozess zu untersuchen und zu bewerten, wie sich Veränderungen in der Organisation auf seine Implementierung auswirken.

… können Sie Messgrößen definieren, die zur Messung des Fortschritts des ISMS erforderlich sind, sowie ein ISMS-Messprogramm entwickeln und verwalten.

… erkennen Sie die Notwendigkeit einer Leistungsbewertung, einschließlich interner Audits des ISMS in Übereinstimmung mit der ISO/IEC 27001 und einer Managementbewertung.

# 4. Kontrolle des Informationssicherheitsmanagementsystems

## Einführung

Nach der Implementierung des Informationssicherheitsmanagementsystems (ISMS) ist es von entscheidender Bedeutung, das System kontinuierlich zu überwachen, zu überprüfen und zu aktualisieren. Die Implementierung ist eine fortlaufende Aufgabe und keine einmalige Aktivität. Daher ist die Überwachung von entscheidender Bedeutung. Neben der Überwachung ist die regelmäßige Messung und Bewertung des Implementierungsfortschritts entscheidend. Dies ermöglicht es der Organisation, die Angemessenheit und Wirksamkeit des ISMS zu überprüfen. Diese Lektion befasst sich mit den Instrumenten zur Messung, Analyse und Bewertung der ISMS-Einführung, einschließlich Beispielen für Kennzahlen zur Messung des Fortschritts.

Ein weiterer wichtiger Aspekt des ISMS-Kontrollmechanismus ist die Bewertung der Leistung des implementierten ISMS, einschließlich interner Audits und Managementbewertungen. Interne Audits sollten regelmäßig durchgeführt werden, um die Wirksamkeit der ISMS-Implementierung zu überprüfen. Diese internen Audits unterscheiden sich von den Audits zur Zertifizierung nach ISO/IEC 27001. Interne Audits des ISMS sind von einem qualifizierten Auditor durchzuführen. Das Ergebnis eines solchen Audits ist ein Bericht, der in der Regel Mängel in der Implementierung aufzeigt und detailliert beschreibt, aufgrund eines Auditprogramms, Auditkriterien und eines mit der Organisationsleitung vereinbarten Plans. Die Überprüfung des ISMS-Fortschritts durch das Management (Managementbewertung) ist ebenfalls ein wichtiger Teil des ISMS-Implementierungsprozesses. Auf diese Weise bringt das Management sein Engagement für den Prozess zum Ausdruck, indem es ihn validiert und gleichzeitig die Effizienz, Wirksamkeit und Angemessenheit der ISMS-Implementierung überprüft.

Die Leistungsbewertung des ISMS und seiner Bestandteile, wie oben beschrieben, wird in dieser Lektion behandelt.

## 4.1 Überwachung, Messung, Analyse und Bewertung

Die ISMS-Implementierung sollte überwacht, gemessen und bewertet werden. Die Leistungsmessung des ISMS ist keine einfache Aufgabe, aber durchaus machbar und wird in den folgenden Unterlernzyklen ausführlich behandelt.

### ISMS-Leistungsbewertung

Nach der Implementierung des ISMS ist es wichtig, das System kontinuierlich zu bewerten, um seine Wirksamkeit und seine Fähigkeit, die Ziele der Organisation und die geschäftlichen Anforderungen angemessen zu erfüllen, zu bestimmen. Die Leistungsbewertung des ISMS ist ein wesentlicher Bestandteil dieses Prozesses. Aber wie kann die Leistung des ISMS gemessen werden?

Von Zeit zu Zeit treten Änderungen auf. Ein gut definierter Änderungsmanagementprozess ermöglicht es der Organisation, Aktualisierungen des bestehenden Frameworks und der operativen Umsetzung des ISMS zu berücksichtigen. Die Verfolgung und Überprüfung von Änderungen ist ein wichtiger Teil des gesamten ISMS-Überwachungsprozesses. Die Überwachung von Vorfällen und neuen Trends und Mustern liefert wertvolle Informationen, um die Aktualisierung des ISMS sicherzustellen und Lücken im System zu berücksichtigen.

Die ISO/IEC 27001:2013 bietet Raum für die Überwachung des ISMS, die unter die Kategorie „Leistungsbewertung“ fällt. Bei der Überwachung und Bewertung des ISMS sollten folgende Aspekte berücksichtigt werden:

* ISMS-Leistung in Bezug auf seine Wirksamkeit, Angemessenheit und Eignung
* Änderungen, Risiken und Auswirkungen und deren Folgen für die Leistung des ISMS
* ISMS-Prozesse und Informationssicherheitsmaßnahmen, um ihre Wirksamkeit, Angemessenheit und Eignung zu überprüfen. Dazu gehören Prozesse für das Incident-Management, die Risikobeurteilung/-behandlung, die Informationsverarbeitung, die Zugangssteuerung und das Personalmanagement.
* Sensibilisierung, Kompetenz und Nutzung des ISMS durch die Mitarbeitenden
* Effizienz, Effektivität und Wirksamkeit der IT- und Netzwerkdienste und -infrastruktur
* Verwaltung von Lieferantenbeziehungen, Dienstleistungen, Verträgen und SLAs
* Übereinstimmung mit den Politiken und Verfahren der Organisation, vertraglichen Verpflichtungen, Gesetzen und Vorschriften

Das ISMS muss überwacht und auf Wirksamkeit und Angemessenheit sowie Eignung überprüft werden.

### ISMS-Messprogramm

Eine Organisation muss festlegen, welche **Kennzahlen** oder Messgrößen sie verwenden wird und wie, wann und von wem oder welche Maßnahmen zur Messung des ISMS getroffen werden.

**Kennzahl**

Dabei handelt es sich um vordefinierte Messgrößen oder Arten von Messgrößen. Eine Messung ist das Ergebnis des Messens einer Sache anhand einer Kennzahl.

Die Auswahl der Messgrößen sollte auf einer gründlichen Überprüfung der ISMS-Leistung hinsichtlich ihrer Angemessenheit, Wirksamkeit und Eignung basieren. Die Leistungsmessung des ISMS ist eine Anforderung der ISO/IEC 27001 und stellt sicher, dass das ISMS seine beabsichtigten Ziele tatsächlich erreicht.

Leistungsindikatoren oder Key Performance Indicators (KPIs) sind Kennzahlen, die verwendet werden, um den Fortschritt bei der Zielerreichung zu messen und zu bewerten. Diese Indikatoren können quantitativer oder qualitativer Art sein. Wirksame KPIs sollten spezifisch, messbar, erreichbar, relevant und zeitgebunden sein. Sie ermöglichen eine datengestützte Entscheidungsfindung zur Leistungsverbesserung. Im Bereich der Informationssicherheit gibt es verschiedene gängige Leistungsindikatoren, die zur Messung herangezogen werden können. Dazu gehören:

* Reaktionszeit bei Sicherheitsvorfällen: Die benötigte Zeit, um einen Sicherheitsvorfall zu erkennen, darauf zu reagieren und ihn zu beheben.
* Mean Time Between Failures (MTBF): Die durchschnittliche Zeit zwischen Sicherheitsvorfällen oder -verletzungen, die Aufschluss über die Wirksamkeit der Präventivmaßnahmen einer Organisation gibt.
* Mean Time To Detect (MTTD): Die durchschnittlich benötigte Zeit zur Entdeckung eines Sicherheitsvorfalls oder einer Sicherheitsverletzung. Eine kürzere MTTD bedeutet, dass potenzielle Bedrohungen effektiv erkannt werden.
* Mean Time To Respond (MTTR): Die durchschnittlich benötigte Zeit, um auf einen Sicherheitsvorfall zu reagieren und ihn zu beheben. Eine kürzere MTTR bedeutet eine schnellere Wiederherstellung und weniger Betriebsunterbrechungen.
* Wirksamkeit von Sicherheitsschulungen und Sensibilisierungsprogrammen: Bewertung der Effektivität von Schulungs- und Sensibilisierungsprogrammen anhand von Faktoren wie Teilnahmequoten, Behalten von Wissen und Verhaltensänderungen.
* Effizienz des Patch-Managements: Messung der Effizienz des Patch-Managements, einschließlich Identifizierung, Test und Bereitstellung von Patches für Software- und Hardware-Schwachstellen.
* Abdeckungsgrad der Risikobewertungen: Prozentsatz der kritischen Assets und Systeme der Organisation, die regelmäßigen Risikobewertungen unterzogen werden, um potenzielle Risiken zu identifizieren und zu mindern.
* Anzahl der Sicherheitsvorfälle: Gesamtzahl der Sicherheitsvorfälle oder -verletzungen in einem bestimmten Zeitraum.
* Prozentsatz der Einhaltung von Sicherheitsrichtlinien und -standards: Grad der Einhaltung der Informationssicherheitspolitiken, -verfahren und -standards der Organisation auf der Grundlage von Auditergebnissen, Richtlinienverstößen und Berichten über die Nichteinhaltung.
* Reifegrad der Sicherheitsmaßnahmen: Bewertung der Wirksamkeit von Sicherheitsmaßnahmen und des Fortschritts bei der Verbesserung des Sicherheitsniveaus im Zeitverlauf.
* Schwachstellenmanagement: Effizienz der Schwachstellenmanagementprozesse der Organisation, einschließlich der Anzahl der identifizierten Schwachstellen, der für ihre Behebung benötigten Zeit und des Prozentsatzes der ungelösten Schwachstellen.

**COBIT 5 für Informationssicherheit**

COBIT 5 umfasst 7 Faktoren für die Steuerung und das Management der IT, darunter auch Prozesse (einschließlich Prozesse für die Informationssicherheit).

* Vergleich der Sicherheitskosten mit dem Budget: Vergleich der tatsächlichen Kosten für Sicherheitsmaßnahmen mit dem Budget für Informationssicherheit zur Ermittlung der Kosteneffizienz.

Die folgenden Leitfäden und Frameworks können bei der Messung der Informationssicherheit hilfreich sein:

* **COBIT 5** für Informationssicherheit ist ein umfassendes Framework, das Organisationen bei der Erreichung ihrer Ziele für die Steuerung und Verwaltung der Unternehmens-IT, einschließlich der Informationssicherheit, unterstützt.
* Die Center for Internet Security (CIS) Security Metrics sind eine Reihe von empfohlenen Metriken für Organisationen zur Bewertung ihrer Sicherheitslage und zur Verfolgung von Verbesserungen im Laufe der Zeit.
* Der Leitfaden zur Leistungsmessung für die Informationssicherheit bietet einen umfassenden Ansatz zur Leistungsmessung für die Informationssicherheit, einschließlich der Festlegung von Zielen, der Auswahl von KPIs und der Überwachung des Fortschritts.

Die Auswahl geeigneter Leistungsindikatoren hängt von der Organisation, ihren individuellen Bedürfnissen und dem Kontext ab. Daher sollten diese Aspekte bereits in den frühen Phasen des ISMS-Implementierungsprozesses bewertet werden. Die Auswahl der richtigen Metrik hängt von der Dynamik und den Anforderungen der Organisation ab. Weitere KPIs könnten die Integration der Informationssicherheit in Projekte, die Einhaltung von IT-Sicherheits- und Architekturstandards, die Reaktion auf Vorfälle und das Problemmanagement umfassen.

Ein effektives ISMS-Messprogramm ist eine wesentliche Komponente eines robusten Informationssicherheits-Governance-Systems. Durch die Auswahl und Überwachung relevanter KPIs können Organisationen wertvolle Erkenntnisse über die Wirksamkeit von Politiken, Prozessen und Maßnahmen gewinnen. Die Verwendung von etablierten Frameworks wie COBIT, CIS Security Metrics und dem Leitfaden zur Leistungsmessung für die Informationssicherheit kann eine solide Grundlage für die Entwicklung eines guten Messprogramms bieten.

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie drei mögliche KPIs, die zur Messung der Leistung eines ISMS verwendet werden.

*COBIT 5 für Informationssicherheit*

*Center for Internet Security (CIS) Security Metrics*

*Leitfaden zur Leistungsmessung für die Informationssicherheit*

1. Bitte markieren Sie die falsche(n) Aussage(n).

* Die Messung der Leistung des ISMS ist eine Anforderung der ISO/IEC 27001.
* Die Auswahl der Metrik muss auf der Überprüfung der ISMS-Leistung im Hinblick auf ihre Angemessenheit, Wirksamkeit und Eignung beruhen.
* Die Konformität zeigt an, dass das ISMS tatsächlich das tut, was es zu leisten beabsichtigt.
* *Die Auswahl der geeigneten Metrik ist nicht abhängig von der Dynamik und den Anforderungen der Organisation.*

1. Bitte vervollständigen Sie den folgenden Satz.

ISO/IEC 27001:2013 bietet Raum für die Überwachung des ISMS, die unter die Überschrift *„Leistungsbewertung“* fällt.

## 4.2 Internes Audit

Audits sind für Organisationen unerlässlich, um die Einhaltung von Vorschriften zu gewährleisten, die Wirksamkeit von Managementsystemen zu bewerten und Prozesse kontinuierlich zu verbessern. Es gibt drei Haupttypen von Audits: 1st-Party-, 2nd-Party- und 3rd-Party-Audits. Jede dieser Arten von Audits dient einem bestimmten Zweck und wird von verschiedenen Parteien durchgeführt.

### 1st-Party-Audits

1st-Party-Audits werden oft von der Organisation selbst durchgeführt, um ihre eigenen Prozesse, Systeme und Aktivitäten anhand einer Reihe von Kriterien zu überprüfen, wie z. B. der ISO/IEC 27001-Norm für ISMS. Ziel solcher Audits ist es, Lücken, Nichtkonformitäten und Verbesserungsmöglichkeiten im Managementsystem der Organisation zu identifizieren. Es gibt drei Arten von internen Audits:

* Compliance-Audits: Diese konzentrieren sich auf die Bewertung der Einhaltung geltender Gesetze, Vorschriften und Richtlinien durch die Organisation.
* Betriebliche Audits: Diese bewerten die Effizienz und Effektivität interner Prozesse, Abteilungen oder Systeme innerhalb der Organisation.
* Vorbereitungsaudits: Diese bewerten die Vorbereitung einer Organisation auf eine externe Zertifizierung (z. B. ISO 27001) und identifizieren Bereiche, die vor einem Zertifizierungsaudit verbessert werden müssen.

### 2nd-Party-Audits

2nd-Party-Audits werden auch als Lieferanten- oder Verkäufer-Audits bezeichnet und werden in der Regel von einer Partei durchgeführt, die ein direktes Interesse an der Organisation hat, wie z. B. Kund:innen, ein Partner oder eine Aufsichtsbehörde. Bei solchen Audits wird die Organisation anhand bestimmter Kriterien oder Anforderungen bewertet, die von einem externen Prüfenden oder im Rahmen einer vertraglichen Vereinbarung festgelegt wurden. Ziel dieser Audits ist es, Vertrauen zu schaffen, Risiken zu mindern und die Leistung der geprüften Organisation zu überwachen. Nachfolgend einige Beispiele für 2nd-Party-Audits:

* Lieferantenqualifikationsaudits: Diese werden von Organisationen durchgeführt, um potenzielle Lieferanten zu bewerten und ihre Fähigkeit zu beurteilen, bestimmte Anforderungen wie Qualität, Sicherheit und Leistung zu erfüllen.
* Vertragskonformitätsaudits: Diese werden von Kund:innen durchgeführt, damit eine Organisation ihren vertraglichen Verpflichtungen nachkommt und die vereinbarten Dienstleistungen oder Produkte liefert.
* Regulatorische Audits: Diese werden von Aufsichtsbehörden durchgeführt, damit eine Organisation die geltenden Gesetze, Vorschriften und Standards einhält.

### 3rd-Party-Audits

3rd-Party-Audits werden in der Regel von unabhängigen externen Organisationen oder Zertifizierungsstellen durchgeführt. Diese Audits dienen zur Bewertung einer Organisation anhand international anerkannter Normen wie ISO/IEC 27001, um zu überprüfen, ob das Managementsystem einer Organisation die Anforderungen der Normen erfüllt. Es soll den Interessengruppen, d. h. Kund:innen, Partnern und Aufsichtsbehörden, die Gewissheit geben, dass die Organisation über ein wirksames Managementsystem verfügt. Nachfolgend sehen Sie einige Beispiele für 3rd-Party-Audits:

* Zertifizierungsaudits: Bei diesem Audit bewertet eine externe Zertifizierungsstelle das Managementsystem einer Organisation anhand einer bestimmten Norm wie z.B. ISO/IEC 27001 und erteilt bei Erfüllung der Anforderungen ein entsprechendes Zertifikat (z. B. ISO/IEC 27001-Zertifikat). Dieses Audit besteht häufig aus zwei Phasen – einer Überprüfung der Dokumentation und einer Bewertung vor Ort.
* Überwachungsaudits: Dabei handelt es sich um regelmäßige, in der Regel jährliche Folgeaudits, die von einer Zertifizierungsstelle durchgeführt werden, um zu überprüfen, ob die Organisation die Standards weiterhin einhält.
* Rezertifizierungsaudits: Dabei handelt es sich um umfassende Audits, die alle drei Jahre durchgeführt werden, um die kontinuierliche Einhaltung der Standards durch eine Organisation zu bestätigen und die Zertifizierung zu erneuern.

Ziel interner ISMS-Audits ist die Überprüfung, inwieweit das ISMS die Anforderungen der Organisation erfüllt. Dabei werden die zugrunde liegenden Prozesse und Teilprozesse der ISMS-Implementierung überprüft, um wichtige Erkenntnisse zur Verbesserung der ISMS-Implementierung zu gewinnen. Dies ist eine wichtige Kontrollaktivität gemäß ISO/IEC 27001, um die Konformität sicherzustellen. Ein Auditprogramm sollte sorgfältig geplant und entwickelt werden. Es sollte die Häufigkeit der Audits, das Verfahren, die Rollen und Verantwortlichkeiten, die Anforderungen, die Berichterstattung und die Definition von Korrektur- und Vorbeugungsmaßnahmen festlegen. Die Audits sollten mindestens alle drei Jahre durchgeführt werden und alle Geschäftsprozesse im Rahmen des ISMS, wie im ISMS-Anwendungsbereich definiert, abdecken. Ein Auditprogramm sollte entwickelt werden, das die Prozesse der Planung, Definition, Durchführung, Überwachung, Überprüfung und Verbesserung des Auditprozesses umfasst.

ISMS-Auditoren sollten Expert:innen sein, die vom Beginn des Auditauftrags bis zur Berichtsphase die erforderliche Objektivität und Neutralität im Auditprozess gewährleisten.

ISMS-Audits sollten so geplant werden, dass nicht konforme Aktivitäten, potenzielle und unerkannte Schwachstellen und Bedrohungen identifiziert werden.

Für die Planung und Durchführung der Audits gelten die folgenden Punkte:

* Audits können erst beginnen, wenn sie in Auftrag gegeben wurden. Der formelle Prozess beginnt mit der Kommunikation mit der auditierten Stelle, wobei der Umfang und andere Aspekte der Auditleistung besprochen und vereinbart werden.
* Während des Auditprozesses sollten die Schritte zur Beseitigung der identifizierten Bedrohungen und Schwachstellen dokumentiert werden.
* Ereignisse aus früheren Audits, wie inhärente Risiken und offene Fragen, sollten entsprechend festgehalten werden.
* Die Ergebnisse des Audits müssen den Beteiligten, einschließlich dem ISMS-Management, mitgeteilt werden. Aus den Berichten muss klar hervorgehen, welche Bereiche auditiert wurden und worauf die Schlussfolgerungen des Audits beruhen.

Das Auditprogramm und die Ergebnisse sollten gemäß Klausel 9.2g der Norm dokumentiert werden.

Es besteht ein Unterschied zwischen den internen Kontrollmechanismen und -systemen einer Organisation und dem ISMS, das als ein Aspekt des gesamten internen Kontrollsystems (IKS) einer Organisation betrachtet wird. Das IKS ist das umfassendere Kontrollsystem auf Organisationsebene, während das ISMS-Audit eine Komponente oder Unterkomponente des gesamten IKS darstellt. Es ist wichtig zu beachten, dass sich ISMS und IKS überschneiden können.

### Fragen zur Selbstkontrolle

1. Bitte vervollständigen Sie den folgenden Satz.

Die Überprüfung von Prozessen und Teilprozessen, die der ISMS-Implementierung zugrunde liegen, um wichtige Beobachtungen zur Verbesserung der ISMS-Implementierung aufzuzeigen, wird in der ISO/IEC 27001:2013 als *„Konformitätsprüfung“* bezeichnet.

1. Bitte vervollständigen Sie den folgenden Satz.

Das organisatorische interne Kontrollsystem (IKS) ist das umfassendere *Kontrollsystem auf organisatorischer Ebene*, während das ISMS-Audit ein *Bestandteil des gesamten IKS* ist.

## 4.3 Managementbewertung

Klausel 9.3 der ISO/IEC 27001 verlangt eine Managementbewertung des ISMS. Die Bewertung soll zwischen den vom Vorstand festgelegten Zeitabständen oder bei einer wesentlichen Änderung des Risikoprofils der Organisation erfolgen. Während der Vorstand oder die Geschäftsführung für die Governance verantwortlich ist, sollte ein:e Informationssicherheitsbeauftragte:r oder eine von der Geschäftsführung benannte Person für die Organisation, Kommunikation und Sammlung von Inputs für den Prozess sowie für die Weiterleitung der Überprüfungsergebnisse an die relevanten Interessengruppen verantwortlich sein.

### Fragen zur Selbstkontrolle

1. Bitte vervollständigen Sie den folgenden Satz.

*Klausel 9.3* der ISO/IEC 27001 verlangt eine Managementbewertung des ISMS.

Zusammenfassung

In dieser Lektion wurde die Leistungsbewertung des ISMS behandelt. Es ist wichtig, den Fortschritt des ISMS zu analysieren und zu bewerten, um seine Wirksamkeit und Effizienz regelmäßig zu überwachen und um auf Veränderungen in der internen Organisation und im externen Umfeld reagieren zu können. Die Metriken zur Messung des Fortschritts des ISMS müssen von der Organisation festgelegt werden, basierend auf ihren individuellen Bedürfnissen und den relevanten Faktoren, die in dieser Lektion behandelt wurden.

Regelmäßige interne Audits des ISMS sollten durchgeführt werden, wobei diese klar von ISO-Zertifizierungsaudits zu unterscheiden sind. Diese Audits haben zum Ziel, die Konformität des ISMS mit den Anforderungen und Vorgaben der ISO/IEC 27001 zu überprüfen, Schwachstellen und Lücken in der Umsetzung des ISMS zu identifizieren und mögliche Verbesserungspotenziale aufzuzeigen.

# Lektion 5 – Verbesserung des Informationssicherheitsmanagementsystems

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… wissen Sie, wie man mögliche Herausforderungen und Nichtkonformitäten bei der Einrichtung des ISMS in einer Organisation angehen kann und können dies erklären.

… sind Sie in der Lage, Maßnahmen zur fortlaufenden Verbesserung des ISMS zu entwickeln.

… können Sie Korrekturmaßnahmen und Pläne für Präventivmaßnahmen planen und umsetzen, damit das ISMS stets ordnungsgemäß funktioniert.

# 5. Verbesserung des Informationssicherheitsmanagementsystems

## Einführung

Bis hierher wurde das ISMS eingerichtet. Die fortlaufende Verbesserung des ISMS ist ein wesentlicher Bestandteil des Implementierungsprozesses und sollte als kontinuierliches Projekt betrachtet werden. Gemäß dem PDCA-Lebenszyklus sollte die Organisation überprüfen, ob die Implementierung auf dem richtigen Weg ist, nicht funktionierende Bereiche anpassen, den Anwendungsbereich neu ausrichten, wenn Probleme auftreten, und Nichtkonformitäten im Prozess beseitigen.

Diese Lektion befasst sich mit dem Umgang mit Nichtkonformitäten, einschließlich der Ursachenanalyse und der Identifizierung und Beseitigung von Implementierungshindernissen und deren häufigsten Ursachen. Es werden Maßnahmen zur fortlaufenden Verbesserung erläutert, um sicherzustellen, dass das ISMS jederzeit wirksam funktioniert und die Informationswerte der Organisation schützt. Darüber hinaus werden Korrektur- und Vorbeugungsmaßnahmen diskutiert, die erforderlich sind, um ein erneutes Auftreten der identifizierten Probleme zu verhindern.

## 5.1 Behandlung von Herausforderungen und Nichtkonformitäten

**Nichtkonformität**

Es gibt schwerwiegende und geringfügige Nichtkonformitäten, die im Rahmen des ISO-Zertifizierungsaudits einer Organisation festgestellt werden können. Schwerwiegende Nichtkonformitäten führen in der Regel zur Verweigerung der Zertifizierung.

Eine **Nichtkonformität** in einem ISMS bedeutet, dass die Anforderungen der ISO/IEC 27001 nicht erfüllt werden. Es ist wichtig zu beachten, dass einige der in der Norm aufgeführten Anforderungen verbindlich sind, während andere als Empfehlungen gelten. Die verbindlichen Anforderungen werden als „Muss“-Anforderungen bezeichnet, die eine Organisation bei der Implementierung eines ISMS und dem Schutz ihrer Informationswerte erfüllen muss. Die meisten Anforderungen in den Normen enthalten das Wort „muss“ und werden bei Audits oder Überprüfungen in die Checkliste für die Einhaltung oder Nichteinhaltung durch die implementierende Einrichtung oder Organisation aufgenommen. Wenn diese Anforderungen nicht erfüllt werden, liegt eine Nichtkonformität vor, die korrigiert werden muss.

Nichtkonformitäten können betrieblicher oder technischer Art sein und durch verschiedene Faktoren oder deren Fehlen verursacht werden. Nachfolgend sehen Sie einige Beispiele:

* Versäumnis des Managements (der Geschäftsführung oder der obersten Leitung), den internen und externen Kontext und die Bedürfnisse aller Stakeholder bei der Einführung des ISMS zu berücksichtigen: Dieses Versäumnis seitens des Managements kann die Wirksamkeit der ISMS-Implementierung beeinträchtigen (Klauseln 4.1 und 4.2 der ISO/IEC 27001:2013).
* Keine klare Definition des Anwendungsbereichs des ISMS: Die Definition des Anwendungsbereichs ist in Klausel 4.3 der ISO/IEC 27001:2013 festgelegt und ist einer der wichtigsten Schritte bei der Einführung eines ISMS. Ohne eine vernünftige Definition des Anwendungsbereichs fehlt es dem ISMS an angemessenen Grenzen, innerhalb derer es umgesetzt werden soll und an denen folglich seine Wirksamkeit gemessen wird.
* Fehlen eines geeigneten Verfahrens zur Risikobeurteilung und Risikobehandlung: Risikobeurteilung und Behandlung sind in Klausel 6 der Normen festgelegt.
* Fortlaufende Verbesserung: Diese muss Teil des ISMS-Implementierungsprozesses sein. Das ISMS ist kein einmaliges Projekt. Das Versäumnis des Managements, sicherzustellen, dass dies als Nichtkonformität angesehen wird, verstößt gegen die Klauseln 5.2 und 6.1.1 der Normen.
* Kleinere Unternehmen und Organisationen stehen oft vor der Herausforderung begrenzter Ressourcen, um den ISMS-Einführungsprozess zu managen, der sowohl personelle als auch materielle Ressourcen erfordert: Gemäß Klausel 7 der Normen liegt die Verantwortung für die Bereitstellung der notwendigen Ressourcen und Unterstützung für die Implementierung des ISMS bei der Unternehmensleitung.
* Versäumnis des Managements, sicherzustellen, dass die Maßnahmen wirksam sind und die in der Anfangsphase der Umsetzung identifizierten Risiken adressieren. Klausel 6 legt angemessene Maßnahmen zur Bewältigung der identifizierten Risiken und die Durchführung von Maßnahmen fest.
* Versäumnis des Managements, die Leistungsbewertung des ISMS sicherzustellen. Die Leistungsbewertung ist in Klausel 9 der Normen festgelegt. Dazu gehören interne Audits und Bewertungen sowie andere Untersuchungen, die dazu beitragen, Herausforderungen bei der ISMS-Implementierung zu identifizieren und zu beheben.

Es liegt in der Verantwortung der Unternehmensleitung, unter anderem durch die Durchführung von Audits, Untersuchungen und Überprüfungen sicherzustellen, dass ordnungsgemäß festgestellte Nichtkonformitäten behoben werden, um eine einwandfreie Implementierung des ISMS zu ermöglichen.

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie vier mögliche Ursachen für Nichtkonformitäten bei der Implementierung eines ISMS.

*Versäumnis des Managements, sicherzustellen, dass die Maßnahmen wirksam sind und die in der Anfangsphase der Umsetzung identifizierten Risiken adressieren.*

*Fehlen eines geeigneten Verfahrens zur Risikobeurteilung und Risikobehandlung.*

*Keine klare Definition des Anwendungsbereichs des ISMS.*

*Versäumnis des Managements (der Geschäftsführung oder der obersten Leitung), den internen und externen Kontext und die Bedürfnisse aller Stakeholder bei der Einführung des ISMS zu berücksichtigen.*

1. Bitte vervollständigen Sie den folgenden Satz.

Die Nichtkonformitäten können *betrieblicher* und *technischer* Art sein.

## 5.2 Fortlaufende Verbesserung

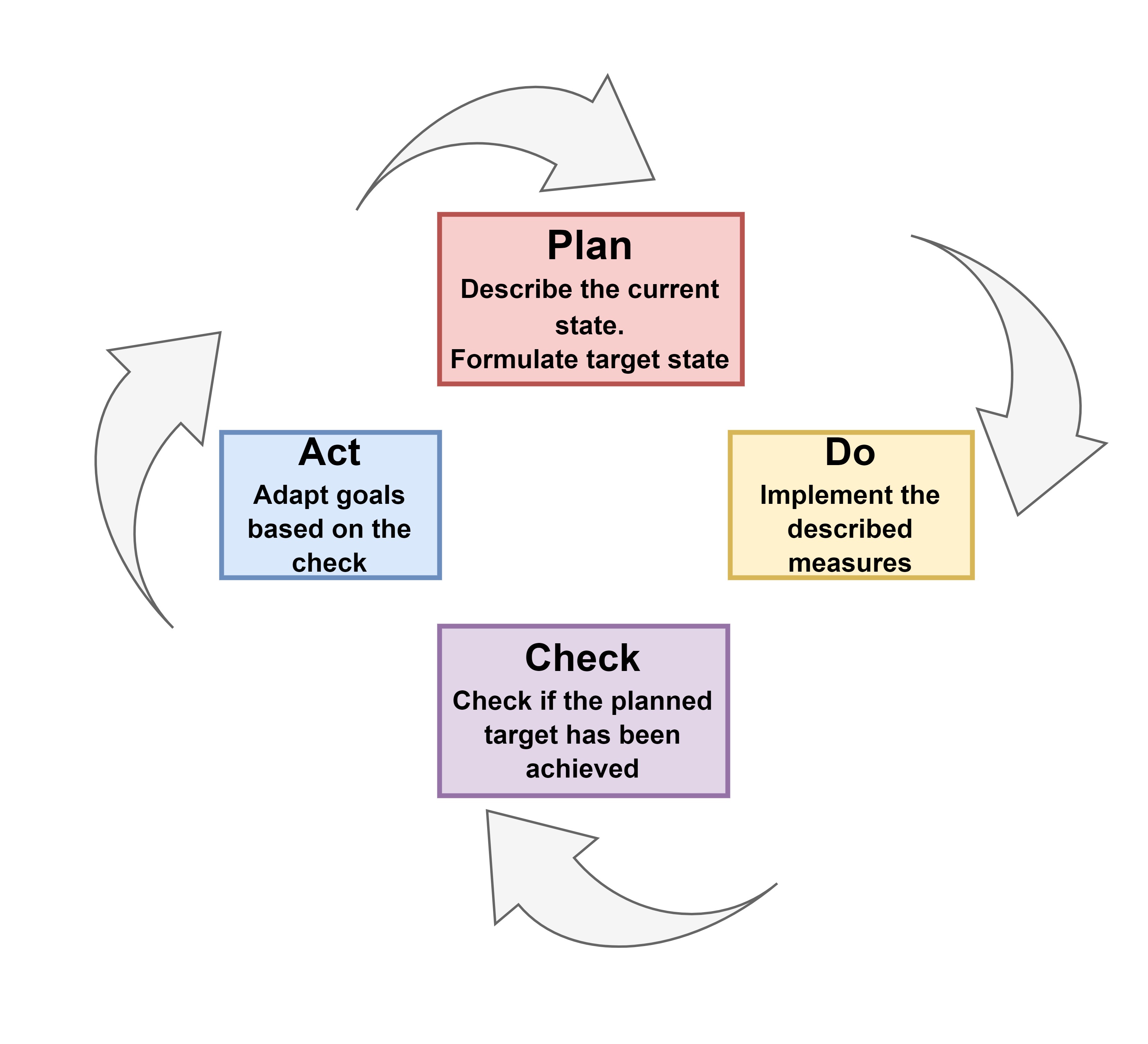
In der ISO/IEC 27001:2013 wird die Verbesserung als „fortlaufende Verbesserung“ bezeichnet und ist als ein Aspekt der Normenkonformität verpflichtend (Humphreys, 2016).

Der **PDCA**-Zyklus (Plan-Do-Check-Act), auch als Deming-Zyklus bekannt, ist ein sehr wertvolles Modell, um die kontinuierliche Verbesserung des ISMS sicherzustellen. Im *Plan*-Schritt wird der aktuelle Zustand des ISMS beschrieben, während im *Do*-Schritt Maßnahmen ergriffen werden, um zu gewährleisten, dass das ISMS wirksam funktioniert. Im *Check-*Schritt wird überprüft, ob das ISMS effektiv und zielgerichtet arbeitet, um die angestrebten Ziele zu erreichen, die sich in die Gesamtziele des Unternehmens einfügen.

**PDCA**

Eine iterative Design- und Managementmethode, die in der Wirtschaft zur Überwachung und fortlaufenden Verbesserung von Prozessen und Produkten eingesetzt wird.

Fortlaufende Verbesserung des ISMS mit PDCA



Quelle: Andrew Sai (2023).

Die Frage, wie Organisationen die Bereiche identifizieren können, die zum Aufbau eines erfolgreichen ISMS verbessert werden müssen, ist von großer Bedeutung. Praktizierende empfehlen häufig die Berücksichtigung der folgenden Bereiche:

* Auditberichte (intern und extern)
* Spezielle und regelmäßige Auditberichte
* Monatliche Leistungsüberprüfungen und -berichte
* Beteiligung oder Berichterstattung durch Mitarbeitende, z. B. Meldung von Vorfällen, wenn Systeme oder Prozesse fehlerhaft sind.
* Managementbewertungsberichte
* Kund:innen und Dritte, sonstige Stakeholder
* Ergebnisse der Überprüfung der Kompatibilität neuer Werkzeuge und Technologien mit bestehenden Systemen und ISMS-Einrichtungen
* Externe Faktoren wie regulatorische und gesetzliche Aktualisierungen

Die obige Liste ist zwar nicht erschöpfend, aber der Erfolg der Verbesserungsschritte kann anhand der in der folgenden Abbildung vorgeschlagenen Vorlage gemessen werden. Verbesserungen könnten in den Bereichen Prozesse, Richtlinien und Verfahren, Sensibilisierung und Schulung erzielt werden. Dieser beispielhafte Tracker (in MS Excel) soll den Organisationsmitgliedern, die das ISMS verbessern wollen, helfen, zu verstehen und zu verfolgen, wie die Verbesserungen in einem bestimmten Zeitraum umgesetzt wurden, wie viel Zeit dafür aufgewendet wurde, wer dafür verantwortlich ist und welche Prioritäten gesetzt wurden.

Vorlage zur Verfolgung eines Plans zur fortlaufenden Verbesserung (Tracker)

Tabelle

Automatisch generierte Beschreibung mit mittlerem Vertrauen

Quelle: Andrew Sai (2023).

### Fragen zur Selbstkontrolle

1. Bitte vervollständigen Sie den folgenden Satz.

Gemäß dem Deming-Zyklus dient *Plan* zur Beschreibung des aktuellen Zustands des ISMS, *Do* zur Umsetzung von Maßnahmen, um zu gewährleisten, dass das ISMS wirksam funktioniert, *Check* zur Sicherstellung, dass das ISMS wirksam und zielgerichtet ist, um das beabsichtigte Ziel zu erreichen, und *Act* zur Durchführung von Änderungen am ISMS nach dessen fortlaufender Überprüfung und Kontrolle.

## 5.3 Pläne für Korrektur- und Präventivmaßnahmen

Wenn Nichtkonformitäten festgestellt wurden, ist die nächste wichtige Maßnahme die Korrektur und anschließend die Vorbeugung, um ein erneutes Auftreten zu vermeiden.

Für Korrekturmaßnahmen ist es wichtig, die Quelle der Anomalie zu identifizieren und sie zu beseitigen. Je nach der Komplexität des Problems oder der Nichtkonformität ist die Durchführung einer **Ursachenanalyse** von größter Bedeutung. Dies hilft zu verstehen, woher das Problem kommt, welche Auswirkungen es hat und wie es eingedämmt werden kann. Die Ursachen können vielfältig sein, z. B. Personal, Prozesse, technische Probleme, Versäumnisse des Managements, methodische Fehler und vieles mehr.

**Ursachenanalyse**

Dies ist eine Problemlösungsmethode, die zur Identifizierung der Grundursachen von Fehlern oder Problemen verwendet wird und in der IT-Branche und Prozessindustrie weit verbreitet ist.

Ein Beispiel für eine solche Nichtkonformität könnte eine fehlerhafte Richtlinie zur Verwaltung von Vermögenswerten und Ausrüstung sein. Diese Anomalie kann behoben werden, indem ein neues Richtliniendokument mit den erforderlichen Änderungen zur Behebung des Problems eingeführt wird. Liegt das Problem darin, dass die Mitarbeitenden nicht ausreichend geschult oder nicht ausreichend darüber informiert sind, wie die Politik oder das Verfahren umzusetzen ist, kann die Nichtkonformität durch zusätzliche Schulungen und Auffrischungskurse für die Mitarbeitenden behoben werden. Ein verbessertes Schulungs- und Sensibilisierungsprogramm kann dazu beitragen, die festgestellte Nichtkonformität zu korrigieren und sicherzustellen, dass das Personal auf dem neuesten Stand ist.

**ISO 22301 – Sicherheit und Resilienz – BCMS**

Hierin wird das Business Continuity Management als Teil des allgemeinen Risikomanagements in einem Unternehmen definiert.

Vorbeugende Aktionspläne begleiten in der Regel die ergriffenen Korrekturmaßnahmen und können von einfachen Schulungsprogrammen bis hin zu größeren Überholungen von Systemen, Prozessen oder mehr reichen, sobald die Problemursache identifiziert und behoben ist. In einigen Fällen, in denen sie nicht behoben werden können und z. B. menschliches Versagen die Hauptursache für ein Problem ist, könnte eine Präventivmaßnahme in der Prozessautomatisierung bestehen, um menschliches Eingreifen auszuschließen.

Im Rahmen der Prävention ist es wichtig, sich vor potenziellen Bedrohungen wie Cyberangriffen, Datenschutzverletzungen und Naturkatastrophen zu schützen, da diese den Geschäftsbetrieb und die Umsetzung des ISMS unterbrechen können. Hier setzt die **ISO/IEC 22301** an, deren Ziel es ist, Organisationen bei der Identifizierung und Priorisierung von Bedrohungen zu unterstützen. Durch die effektive Implementierung eines Business Continuity Management Systems (BCMS) sind Organisationen besser auf solche Vorfälle vorbereitet. Sie können sich schneller erholen und den Geschäftsbetrieb mit minimaler Unterbrechung aufrechterhalten im Vergleich zu Organisationen, die nicht mit BCMS-Standards arbeiten.

### Fragen zur Selbstkontrolle

1. Bitte markieren Sie die falsche(n) Aussage(n).

* Wenn Nichtkonformitäten entdeckt wurden, ist die nächste wichtige Maßnahme die Korrektur.
* Die Ursachen können vielfältig sein, z. B. Personal, Prozesse, technische Probleme, Versäumnisse des Managements oder methodische Fehler.
* Präventive Aktionspläne begleiten in der Regel die ergriffenen Korrekturmaßnahmen.
* *Eine fehlerhafte Politik ist kein Beispiel für eine Nichtkonformität.*

Zusammenfassung

In der Lektion wurden zuerst die Nichtkonformitäten besprochen, dann die fortlaufende Verbesserung und die für die Problembehebung notwendigen Korrektur- und Präventionsmaßnahmen. Nichtkonformitäten beziehen sich auf die Nichterfüllung von in den Normen festgelegten Anforderungen. Es ist von größter Wichtigkeit, dass das Management einer Organisation Nichtkonformitäten ernst nimmt und wirksame Maßnahmen zur Verbesserung des ISMS ergreift. Sobald Nichtkonformitäten erkannt werden, sollten unverzüglich Schritte zur Verbesserung des ISMS eingeleitet werden. Kontinuierliche Überwachung ist dabei entscheidend. Das Management ist dafür verantwortlich, Bereiche mit Verbesserungspotenzial zu identifizieren, sodass die Implementierung des ISMS erfolgreich ist.

# Lektion 6 – Maßnahmen des Informationssicherheitsmanagementsystems

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… können Sie die allgemeine Struktur der in der ISO/IEC 27000-Normenreihe aufgeführten Maßnahmen identifizieren und erörtern, insbesondere die ISO/IEC 27001 und ISO/IEC 27002.

… sind Sie in der Lage, die in Anhang A der ISO/IEC 27001 vorgeschriebenen Gruppierungen und Kategorisierungen der verschiedenen Maßnahmen nachzuvollziehen und zu beschreiben.

… können Sie die Maßnahmen, die im Rahmen der ISMS-Implementierung eingeführt wurden, unterscheiden und verwalten.

… sind Sie in der Lage, die Wirksamkeit der Maßnahmen des ISMS in einer Organisation zu bewerten und ggf. Maßnahmenziele zu formulieren, die den Anforderungen der Organisation entsprechen.

# 6. Maßnahmen des Informationssicherheitsmanagementsystems

## Einführung

Anhang A der ISO/IEC 27001 enthält wichtige Maßnahmen, die Elemente des Risikomanagements darstellen und auf der Grundlage einer umfassenden Risikobeurteilung in einer Organisation sorgfältig ausgewählt werden müssen. Vor der Umsetzung dieser Maßnahmen, müssen die Risiken beurteilt, die Geschäftsanforderungen und Best Practices geprüft und die gesetzlichen sowie die vertraglichen Verpflichtungen analysiert werden.

**ISO-Zertifizierung**

Diese Zertifizierung belegt, dass sich eine Organisation für die kontinuierliche Verbesserung, Entwicklung und den Schutz von Informationsbeständen und Daten durch die Implementierung von Risikobeurteilungen, Politiken und Maßnahmen einsetzt.

Die Maßnahmen im Anhang A der ISO/IEC 27001 sind in verschiedene Kategorien unterteilt. Eine detaillierte Erläuterung dieser Maßnahmen findet sich in ISO/IEC 27002. Die ursprünglich 14 Klauseln der ISO/IEC 27001:2013 wurden in der Ausgabe von 2022 durch vier Themenbereiche ersetzt und die Anzahl der Maßnahmen von 114 auf 93 reduziert. Diese Aktualisierungen sind lediglich Umstrukturierungen des gleichen Inhalts und haben keinen Einfluss auf die Kernstruktur der ISO-Normenfamilie. Dennoch sind diese Aktualisierungen von entscheidender Bedeutung für Organisationen, die eine **Rezertifizierung nach ISO/IEC 27001** anstreben.

In dieser Lektion wird ausgiebig auf die ISO/IEC 27001:2013 und die ISO/IEC 27002:2013 verwiesen. Wo Inhalte aus der aktualisierten Version der ISO/IEC 27001 oder 27002:2022 gemeint sind, werden sie ausdrücklich angegeben.

Die aus der Liste in Anhang A der ISO/IEC 27001 ausgewählten Maßnahmen müssen eine detaillierte Begründung für ihre Aufnahme oder ihren Ausschluss enthalten. Diese Begründung basiert in der Regel auf Faktoren, die im Umfeld der Organisation, welche das ISMS einführt, relevant sind. Die Erklärung zur Anwendbarkeit (Statement of Applicability, SoA) dokumentiert die Gründe für die Aufnahme oder den Ausschluss bestimmter Maßnahmen. Die SoA bietet dem Management eine Momentaufnahme der Risikoexposition, des Risikoniveaus und des Fortschritts der Risikobehandlung.

Die Lektion behandelt zunächst den allgemeinen Begriff „Maßnahmen“ und fasst die in ISO/IEC 27001 aufgeführten Maßnahmenkategorien und ihre Ziele zusammen. Abschließend wird erörtert, wie Maßnahmen verwaltet und bewertet werden sollten, um ihre Angemessenheit und Wirksamkeit zu überprüfen.

## 6.1 Allgemeine Struktur von Maßnahmen

Maßnahmen sind die Methoden, Systeme und Prozesse, die eine Organisation einsetzt, um ihre Untereinheiten und Mitglieder zu ermutigen, in Übereinstimmung mit den Erlassen und Vorschriften der Organisation zu handeln. Diese Maßnahmen können Regeln, Richtlinien, Verfahren, Politiken und andere Instrumente sein, welche die Art und Weise der Umsetzung von Dingen innerhalb der Organisation steuern.

Im Kontext des ISMS sind Maßnahmen Schritte zur Reduzierung von Risiken und Bedrohungen für die Informationswerte einer Organisation. Solche Maßnahmen sind häufig in Normen vorgeschrieben.

Die Umsetzung von Maßnahmen erfolgt im Rahmen des Risikomanagementprozesses. Es ist wichtig zu beachten, dass die ISO/IEC 27001 als Managementsystemnorm für den Schutz von Informationen und nicht ausschließlich als IT-Sicherheitsnorm konzipiert ist. Daher liegt der Schwerpunkt häufig auf managementorientierten Ansätzen.

Einige Beispiele für Maßnahmen innerhalb einer Organisation sind Informationssicherheitspolitik, Einstellungsverfahren, Internetnutzungspolitik, Zugangskontrollpolitik, Kommunikationspolitik, Sicherheitsverfahren, Standardbetriebsverfahren, Vorfallsmanagementverfahren und andere.

**Maßnahmen-Framework**

Hierbei handelt es sich um eine Datenstruktur, welche die internen Maßnahmen einer Organisation organisiert und kategorisiert, einschließlich der Praktiken und Verfahren, die zur Schaffung von Geschäftswerten und zur Verringerung von Risiken eingerichtet wurden.

Die oben genannten Maßnahmen könnten in Form eines **Maßnahmen-Frameworks** in Pakete aufgeteilt werden, die aus folgenden Elementen bestehen könnten

* Politiken und Verfahren
* Prozesse
* Praktiken
* Pläne
* Programme

Jedes der Maßnahmenelemente kann in einem dieser Pakete enthalten sein.

In der ISO/IEC 27001:2022 gibt es die folgenden vier Hauptbereiche für Maßnahmen:

Organisatorische Maßnahmen

Menschliche Maß nahmen

Physische Maßnahmen

Technologische Maßnahmen

ISO/IEC 27001 – Bereiche für Maßnahmen

Quelle: Andrew Sai (2023).

Diese vier Bereiche wurden in die aktualisierte Version von ISO/IEC 27001:2022 aufgenommen. Die Themen wurden eingeführt, um die Maßnahmen entsprechend zu gruppieren. Auch hier handelt es sich um eine Neuorganisation bzw. Aufbereitung dessen, was bereits in der ISO/IEC 27001:2013 enthalten war:

* Organisatorische Maßnahmen (37 Maßnahmen): Dabei handelt es sich um Maßnahmen für die Einrichtung wichtiger organisatorischer Sicherheitsprozesse und deren Dokumentation, wie z. B. organisatorische Informationspolitiken, die Nutzung von Cloud-Diensten, die Nutzung von Assets und mehr.
* Personalmaßnahmen (8 Maßnahmen): Dies sind Maßnahmen für ein sicheres Personalmanagement in Organisationen, einschließlich Telearbeit, Vertraulichkeit, Geheimhaltung und Überprüfung.
* Physische Maßnahmen (14 Maßnahmen): Dies sind die Maßnahmen zur Sicherung von Bereichen und Geräten in der Organisation, einschließlich Sicherheitsüberwachung, Speichermedien, Wartung und Anlagensicherheit.
* Technologische Maßnahmen (34 Maßnahmen): Dabei handelt es sich um Maßnahmen zum Schutz von IT- und Kommunikationssystemen, einschließlich Maßnahmen zur Authentifizierung, Verschlüsselung und Verhinderung von Datenverlust.

Die Änderungen an der ISO/IEC 27000-Normenfamilie finden sich auf der ISO-Website (ISO, 2022). In der Ausgabe 2022 wurden 11 neue Maßnahmenkategorien hinzugefügt, darunter Bedrohungsanalyse, Informationssicherheit für die Nutzung von Cloud-Diensten, IKT-Bereitschaft für die Geschäftskontinuität, Konfigurationsmanagement, Informationslöschung, Datenmaskierung, Verhinderung von Datenlecks, Überwachungsaktivitäten, Web-Filterung und sichere Codierung. Außerdem wurden neue Attribute eingeführt, um die Kategorisierung von Maßnahmen in der Norm zu erleichtern:

* Art der Maßnahme (präventiv, detektivisch, korrigierend)
* Eigenschaften der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit)
* Konzepte der Cybersicherheit (identifizieren, schützen, erkennen, reagieren und wiederherstellen)
* operative Kapazitäten (Governance, Asset-Management usw.)
* Sicherheitsbereiche (Governance und Ökosystem, Schutz, Verteidigung, Resilienz)

### Fragen zur Selbstkontrolle

1. Bitte nennen Sie mindestens drei der Elemente, die in einem Maßnahmen-Framework enthalten sein könnten.

* *Politiken und Verfahren*
* *Prozesse*
* *Praktiken*
* *Pläne*
* *Programme*

1. Welcher der folgenden Bereiche gehört nicht zu den vier Bereichen, die in die aktualisierte Version der ISO/IEC 27001:2022 aufgenommen wurden?

* *Geschäftliche Maßnahmen*
* Technologische Maßnahmen
* Physische Maßnahmen
* Personalmaßnahmen

1. Bitte vervollständigen Sie den folgenden Satz.

Diese Maßnahmen können *Regeln*, *Richtlinien*, *Verfahren*, *Politiken* und andere Instrumente sein, die die Art und Weise steuern, wie Dinge innerhalb der Organisation umgesetzt werden.

## 6.2 Maßnahmen der ISO/IEC 27001 – Anhang A

**Anhang A der ISO/IEC 27001**

Dies ist der bekannteste Teil der ISO-Normen. Er ist ein wichtiges Instrument für das Management von Informationssicherheitsrisiken und bietet eine Liste von Sicherheitsmaßnahmen, die zur Verbesserung der Sicherheit in einer Organisation erforderlich sind.

**Anhang A** **der ISO/IEC 27001**-Normenenthält wesentliche Maßnahmen für das Management von Informationssicherheitsrisiken in einer Organisation. Er enthält eine Liste von Maßnahmen oder Sicherheitsvorkehrungen, die zur Stärkung der Informationssicherheit einer Organisation erforderlich sind. Anhang A enthält eine Zusammenfassung aller Maßnahmen, die in der ISO/IEC 27002 detailliert beschrieben und erläutert werden. Es werden auch Hinweise zur Umsetzung dieser Maßnahmen gegeben. Damit wird der Zusammenhang zwischen ISO/IEC 27001 und ISO/IEC 27002 deutlich.

Wie bereits erwähnt, ist Anhang A der ISO/IEC 27001:2013 in 14 Maßnahmenkategorien unterteilt. In der ursprünglichen Fassung beinhaltete der Anhang 114 Maßnahmen, in der aktualisierten Fassung ISO/IEC 27001:2022 wurde die Anzahl der Maßnahmen auf 93 reduziert. Die Einteilung der Maßnahmen in 14 Gruppen erleichtert die Identifizierung der verschiedenen Maßnahmenbereiche und trägt zur Verbesserung der Informationssicherheit in Organisationen bei. Diese folgen einer festgelegten Struktur mit einer Namenskonvention. Jede der 14 Maßnahmenkategorien wird im Folgenden zusammengefasst und beschrieben, wobei die Namen/Nummern der Kategorien und die Anzahl der Ziele und Maßnahmen in jeder Kategorie angegeben werden. Die Ziele werden kurz behandelt; für eine detaillierte Darstellung der Maßnahmen kann direkt die ISO-Website konsultiert werden. Nachfolgend sind die Zusammenfassungen und Beschreibungen der Maßnahmenkategorien aus Anhang A der ISO/IEC 27001:2013 (ISACA, 2017) aufgeführt:

* **Informationssicherheitspolitiken** (Maßnahmenkategorie A.5 – 1 Ziel und 2 Maßnahmen): Diese Kategorie gibt die Richtung für das Management vor und bietet Unterstützung bei der Erfüllung organisatorischer und rechtlicher Anforderungen.
* **Informationssicherheitsorganisation** (Maßnahmenkategorie A.6 – 3 Ziele und 6 Maßnahmen): Diese Kategorie schafft einen Managementrahmen für die Implementierung und den Betrieb der Informationssicherheit, einschließlich der Sicherheit von Telearbeit und mobilen Endgeräten.
* **Personalsicherheit** (Maßnahmenkategorie A.7 – 3 Ziele und 6 Maßnahmen): Diese Kategorie befasst sich mit den Anforderungen vor der Einstellung, der Sicherstellung der Verantwortung der Mitarbeitenden für die Informationssicherheit während der Beschäftigung und dem Schutz der Organisationsinteressen beim Wechsel von Mitarbeitenden.
* **Asset Management** (Maßnahmenkategorie A.8 – 3 Ziele und 10 Maßnahmen): Diese Kategorie identifiziert Informationswerte, legt Verantwortlichkeiten für die Sicherung fest und schützt Informationen vor unbefugter Offenlegung, Aktualisierung oder Zerstörung.
* **Zugangssteuerung** (Maßnahmenkategorie A.9 – 4 Ziele und 14 Maßnahmen):Diese Kategorie beschränkt den Zugang zu Informationen und Verarbeitungseinrichtungen, ermöglicht den Zugang für autorisierte Benutzer:innen, fördert die Sicherheit von Passwörtern und PINs und verhindert den unbefugten Zugang zu Systemen und Anwendungen.
* **Kryptografie** (Maßnahmenkategorie A.10 – 1 Ziel und 2 Maßnahmen):Diese Kategorie befasst sich mit dem Einsatz von Kryptografie zum Schutz von Informationswerten.
* **Physische und Umgebungssicherheit** (Maßnahmenkategorie A.11 – 2 Ziele und 15 Maßnahmen):Diese Maßnahmenkategorie verhindert den unbefugten physischen Zugriff auf Informationswerte und -einrichtungen und schützt die Organisation vor Verlust, Diebstahl oder Betriebsunterbrechung.
* **Betriebssicherheit** (Maßnahmenkategorie A.12 – 7 Ziele und 14 Maßnahmen): Diese Kategorie stellt sicher, dass Informationswerte und physische Standorte geschützt werden; Schutz vor Schadsoftware, Schutz vor Datenverlust, einschließlich Backups und Richtlinien und Verfahren zur Sicherung von Backups; Aufzeichnung von Ereignissen und Bereitstellung von Beweisen, wo dies erforderlich ist; Integrität der operativen Systeme; Verhinderung der Ausnutzung technischer Schwachstellen; und schließlich Verringerung der Auswirkungen von Audit-Aktivitäten auf die operativen Systeme in einer Organisation.
* **Kommunikationssicherheit** (Maßnahmenkategorie A.13 – 2 Ziele und 7 Maßnahmen): Diese Kategorie bezieht sich auf die Pflege der intern und extern übermittelten Informationen.
* **Beschaffung, Entwicklung und Wartung von Systemen** (Maßnahmenkategorie A.14 – 3 Ziele und 13 Maßnahmen): Diese Kategorie bezieht sich auf eine Reihe von Maßnahmen, die sicherstellen, dass die Informationssicherheit ein zentraler Bestandteil von Informationssystemen ist, u. a. über öffentliche Netzwerke, Design und Entwicklung von Informationssystemen innerhalb des Entwicklungslebenszyklus und die Gewährleistung des Schutzes von Daten, die beim Testen von Software im Laufe ihrer Entwicklung verwendet werden, einschließlich ihrer Anonymisierung.
* **Lieferantenbeziehungen** (Maßnahmenkategorie A.15 – 2 Ziele und 5 Maßnahmen): Diese Kategorie dient dem Schutz von Assets, die für Lieferanten und Dritte zugänglich sind, sowie der Aufrechterhaltung des vereinbarten Niveaus der Informationssicherheit und der Servicebereitstellung gemäß den Vereinbarungen mit diesen Lieferanten.
* **Handhabung von Informationssicherheitsvorfällen** (Maßnahmenkategorie A.16 – 1 Ziel und 7 Maßnahmen): Soll die ordnungsgemäße Handhabung von Sicherheitsvorfällen gewährleisten, einschließlich der Kommunikation von Sicherheitsvorfällen und Schwachstellen.
* **Informationssicherheitsaspekte im Rahmen des Business Continuity Managements** (Maßnahmenkategorie A.17 – 2 Ziele und 4 Maßnahmen): Zur Vermeidung von Verstößen gegen rechtliche, gesetzliche, behördliche und vertragliche Anforderungen an die Informationssicherheit und deren Verpflichtungen; zur Gewährleistung der Verfügbarkeit von Informationsverarbeitungsstandorten.
* **Compliance** (Maßnahmenkategorie A.18 – 2 Ziele und 8 Maßnahmen): Zur Vermeidung von Verstößen gegen rechtliche, gesetzliche, behördliche und vertragliche Anforderungen an die Informationssicherheit und um sicherzustellen, dass die Praktiken der Informationssicherheit mit den Richtlinien und Verfahren der Organisation übereinstimmen.

Für jede der in Anhang A der ISO/IEC 27001:2013 aufgeführten Maßnahmenkategorien werden die spezifischen Maßnahmen in der ISO/IEC 27002:2013 oder ihren aktualisierten Fassungen, wie z. B. ISO/IEC 27001:2022 und ISO/IEC 27002:2022, detaillierter beschrieben.

### Fragen zur Selbstkontrolle

1. Anhang A der ISO/IEC 27001:2013 listet auf:

* *114 Maßnahmen und 14 Maßnahmenkategorien*
* 14 Maßnahmen und 114 Maßnahmenkategorien
* 37 Maßnahmen und 93 Maßnahmenkategorien
* 93 Maßnahmen und 37 Maßnahmenkategorien

1. Bitte nennen Sie fünf Maßnahmenkategorien der ISO/IEC 27001:2013-.

*Informationssicherheitspolitiken*

*Personalsicherheit*

*Zugangssteuerung*

*Kryptografie*

*Compliance*

## 6.3 Maßnahmenmanagement

Ein effektives Maßnahmenmanagement ist ein entscheidender Aspekt bei der Einführung, Pflege und Verbesserung eines ISMS. Wenn Organisationen Maßnahmen in ihrem ISMS einführen oder anpassen, wird dringend empfohlen, eine Gap-Analyse durchzuführen, um die Angemessenheit der Maßnahmen zur Erfüllung der Anforderungen des ISMS zu bewerten. Die Ergebnisse der Gap-Analyse sind wertvoll für die Aktualisierung von Politiken, Prozessen und die allgemeine Verbesserung des ISMS. Die Entscheidung, welche Maßnahmen umgesetzt werden, hängt stark von den spezifischen Anforderungen, der Branche und den Zielen der Organisation ab. In diesem Lernzyklus werden verschiedene Aspekte des Kontrollmanagements beschrieben, einschließlich der Auswahl geeigneter Maßnahmen, der Dokumentation, der Personalschulung und der kontinuierlichen Überwachung und Verbesserung.

### Geeignete Maßnahmen auswählen

Organisationen müssen die Maßnahmen auswählen, die für ihre Tätigkeiten und die Umsetzung des ISMS am wichtigsten sind. Maßnahmen, die nicht für den Tätigkeitsbereich oder die Branche der Organisation relevant sind, können ausgeschlossen werden, vorausgesetzt, dass der Ausschluss begründet und in einer SoA dokumentiert wird, in der detailliert dargelegt wird, warum die ausgewählte Maßnahme angesichts der spezifischen Ziele, Anforderungen und Umstände der Organisation nicht erforderlich ist. Wenn eine Organisation z. B. keine Software entwickelt, kann sie sich dafür entscheiden, Maßnahmen im Zusammenhang mit dem Entwurf und der Entwicklung von Informationssystemen innerhalb eines vorgeschriebenen Softwareentwicklungszyklus (Maßnahmenkategorie A.14 - Beschaffung, Entwicklung und Wartung von Systemen) auszuschließen. Ein solcher Ausschluss muss jedoch begründet und in der SoA dokumentiert werden, um zu verdeutlichen, warum diese spezifische Maßnahme nicht erforderlich ist.

### Dokumentation

Eine ordnungsgemäße Dokumentation spielt eine entscheidende Rolle bei der Verwaltung der Maßnahmen eines ISMS. Sie muss wesentliche Informationen über die analysierten Risiken, die ausgewählten Maßnahmen, die Gründe für die Aufnahme oder den Ausschluss von Maßnahmen, die Verantwortlichkeiten und Details über die Wirksamkeit der Maßnahmen und deren Umsetzung enthalten. Die Dokumentation ist für das Management von großer Bedeutung, um die Gründe für die einzelnen Maßnahmen und ihre Auswirkungen auf das gesamte ISMS zu verstehen. Sie dient auch als solide Grundlage für die Verbesserung und Feinabstimmung des Systems. Die Dokumentation dient nicht nur organisatorischen Zwecken, sondern ist auch eine Voraussetzung für die Zertifizierung nach ISO/IEC 27001. Eine angemessene und effiziente Dokumentation ermöglicht es, Maßnahmen zu identifizieren und zu verfolgen und geeignete Schritte zur Behebung von Nichtkonformitäten oder Problemen einzuleiten.

### Schulung des Personals

Die Schulung des Personals ist ein weiterer wichtiger Aspekt des Maßnahmenmanagements. Es muss sichergestellt werden, dass die Mitarbeitenden, die direkt an der Umsetzung des ISMS beteiligt oder für die Überwachung der Umsetzung verantwortlich sind, über die notwendigen Fähigkeiten, Kenntnisse und Kompetenzen verfügen, um die Wirksamkeit des ISMS zu gewährleisten. Die Schulung sollte auf die Bedürfnisse der Organisation zugeschnitten sein und unter anderem folgende Themen abdecken:

* Überblick über das ISMS
* spezifische Politik und Verfahren der Organisation
* relevante Maßnahmen
* Berichterstattung von und Reaktion auf Vorfälle
* Sicherheitsbewusstsein und -kultur

Die Schulung des Personals ist eine wichtige Voraussetzung für die ISO/IEC-Zertifizierung und die Einhaltung der Normen. Organisationen sollten ihre Schulungsprogramme regelmäßig überprüfen und anpassen, um den sich entwickelnden Anforderungen an die Informationssicherheit, den Risiken und den gesetzlichen Anforderungen gerecht zu werden.

### Fortlaufende Überwachung und Verbesserung

Ein wirksames Maßnahmenmanagement beinhaltet die fortlaufende Überwachung, Bewertung und Verbesserung der Maßnahmenleistung. Die Implementierung von Überwachungsmechanismen, wie z. B. regelmäßige Audits und Konformitätsbewertungen, ist entscheidend, damit die ausgewählten Maßnahmen weiterhin relevant, angemessen und ausreichend sind, um die Bedürfnisse der Organisation und die Ziele des ISMS zu erfüllen. Die Integration von Feedbackschleifen in das System ermöglicht fortlaufendes Lernen und Verbesserungen, was wesentlich zum Erfolg des ISMS beiträgt. Das Feedback kann aus verschiedenen Quellen stammen, z. B. von Mitarbeitenden, Kund:innen, Lieferanten, Auditoren und Aufsichtsbehörden. Die Ergebnisse dieser Überwachungsaktivitäten sollten Organisationen bei der Umsetzung oder Verbesserung von Korrektur- und Präventivmaßnahmen unterstützen.

Zusammenfassend kann gesagt werden, dass das Maßnahmenmanagement ein wichtiger Aspekt bei der Implementierung und Pflege eines ISMS ist. Die Auswahl geeigneter Maßnahmen, eine angemessene Dokumentation, die Schulung des Personals sowie die fortlaufende Überwachung und Verbesserung des Systems tragen alle dazu bei, die Sicherheit einer Organisation zu verbessern und die Einhaltung der ISO/IEC 27001 zu gewährleisten.

### Fragen zur Selbstkontrolle

1. Bitte vervollständigen Sie den folgenden Satz.

Im Rahmen des Maßnahmenmanagements wird erwartet, dass nicht umgesetzte Maßnahmen in eine *Anwendbarkeitserklärung* oder *SoA* aufgenommen werden.

## 6.4 Bewertung der Wirksamkeit der Maßnahmen

Im Bereich des Risikomanagements und der internen Kontrollsysteme spielt die Bewertung der Wirksamkeit der Maßnahmen eine entscheidende Rolle, um die Gesamteffizienz und Zuverlässigkeit der Organisation zu gewährleisten. Angesichts der dynamischen Herausforderungen und Risiken, mit denen Unternehmen konfrontiert sind, wird es immer wichtiger, die Stärken und Schwächen der bestehenden Kontrollmaßnahmen zu bewerten. In diesem Unterlernzyklus werden verschiedene Methoden, Kriterien und Indikatoren untersucht, die bei der Bewertung der Wirksamkeit von Maßnahmen für Organisationen mit einem robusten Kontrollumfeld verwendet werden.

Maßnahmen können viele Formen annehmen, von Richtlinien, Prozessen und Praktiken bis hin zu Technologien und Methoden. Sie können präventive, aufdeckende oder korrigierende Funktionen haben. Wirksame Maßnahmen tragen zur Risikominderung bei. Die internen Kontrollmechanismen einer Organisation sollten regelmäßig überprüft werden, um ihre Wirksamkeit festzustellen. Die Beurteilung der Wirksamkeit einer Maßnahme kann anhand verschiedener Faktoren erfolgen:

* Die Relevanz der Maßnahme (Deckt sie die identifizierten Risiken ab?)
* Die Vollständigkeit der Maßnahme (Deckt sie alle Risiken ab, die behandelt werden sollen?)
* Die Zuverlässigkeit der Maßnahme (Funktioniert sie wie erwartet?)
* Die zeitliche Dimension der Maßnahme (Wird sie zum richtigen Zeitpunkt durchgeführt?)

Bei der Bewertung der Wirksamkeit einer Maßnahme ist es wichtig zu prüfen, ob sie dazu beiträgt

* die Auswirkungen von Risiken zu verringern.
* die Wahrscheinlichkeit des Risikoeintritts zu verringern.
* mögliche Angriffe zu erkennen und darauf zu reagieren, bevor sie sich materialisieren.
* Korrektur- und Präventivmaßnahmen zu ergreifen.

Um die Eignung, Angemessenheit und Wirksamkeit eines ISMS zu überprüfen, können verschiedene Methoden angewendet werden. Unabhängig von der gewählten Methode ist es jedoch wichtig zu gewährleisten, dass Risiken, welche die Ziele der Organisation ernsthaft gefährden könnten, identifiziert, bewertet und gemindert werden.

Daten spielen in jedem Bewertungsprozess eine wesentliche Rolle, und dies gilt auch für die Bewertung der Wirksamkeit von Maßnahmen. Solche Daten, ob qualitativ oder quantitativ, können aus verschiedenen Quellen stammen, wie z. B. Beschwerden und Umfrageergebnisse, gemeldete Vorfälle, Ursachen- und Problemanalysen, Berichte von Nutzer:innen, Selbstbewertungsberichte, Auditberichte usw.

Zur Bewertung der Wirksamkeit von Maßnahmen wird häufig eine Skala verwendet, die in der Regel 3 oder 5 Stufen umfasst. Bei einer dreistufigen Skala könnten die Stufen z.B. wie folgt aussehen:

* wirksam (Stufe 3)
* teilweise wirksam (Stufe 2)
* unwirksam (Stufe 1)

Stufe 3 bedeutet, dass die Maßnahmen wirksam sind und wie erwartet funktionieren. Stufe 1 deutet darauf hin, dass die Maßnahmen nicht gut funktionieren, nicht ordnungsgemäß dokumentiert oder kommuniziert wurden, basierend auf den entwickelten Kriterien. Eine fünfstufige Skala könnte wie folgt aussehen:

* voll wirksam (Stufe 5)
* im Wesentlichen wirksam (Stufe 4)
* teilweise wirksam (Stufe 3)
* weitgehend unwirksam (Stufe 2)
* völlig unwirksam (Stufe 1)

Unabhängig von der verwendeten Skala ist es wichtig, dass ein konsistentes und gemeinsames Verständnis darüber besteht, wie und wann die Wirksamkeit von Maßnahmen bewertet wird. Unwirksame Maßnahmen können zu größeren Risiken und Gefahren für die Organisation führen.

Zusammenfassend kann gesagt werden, dass die Bewertung der Wirksamkeit von Maßnahmen eine wesentliche Komponente zur Aufrechterhaltung eines starken Kontrollumfelds und zur Risikominderung ist. Ein umfassender und systematischer Ansatz, der alle Aspekte des Kontrollsystems einbezieht, ermöglicht es, Bereiche mit Verbesserungspotenzial zu identifizieren. Ein gut konzipiertes und effektiv funktionierendes Kontrollsystem bildet letztendlich die Grundlage für eine resiliente und erfolgreiche Organisation.

### Fragen zur Selbstkontrolle

1. Bitte markieren Sie die falsche(n) Aussage(n).

Bei der Beurteilung der Wirksamkeit der Maßnahmen ist es wichtig zu bewerten, ob die Maßnahmen hilfreich sind zur:

* Reduzierung der Auswirkungen von Risiken.
* Verringerung der Wahrscheinlichkeit von Risiken.
* Erkennung möglicher Angriffe und Reaktion darauf, bevor sie sich materialisieren.
* *Reduzierung von Korrektur- und Präventivmaßnahmen.*

1. Bitte vervollständigen Sie den folgenden Satz.

Auf einer dreistufigen Bewertungsskala für Maßnahmen bedeutet Stufe 3, dass die *Maßnahmen wirksam sind und wie erwartet funktionieren*, während Stufe 1 bedeutet, dass die *Maßnahmen nicht gut funktionieren*, *nicht gut dokumentiert* sind oder *nicht gut kommuniziert* werden.

Zusammenfassung

Die Maßnahmen können in individuellen Paketen organisiert werden, die auf dem spezifischen Kontrollrahmen einer Organisation basieren, der zur Pflege ihres Informationssicherheitssystems entwickelt wurde. Diese Maßnahmenpakete umfassen Politiken, Verfahren, Pläne und Programme.

Anhang A der ISO/IEC 27001:2013 enthält eine Liste von 14 Maßnahmenkategorien und 114 Maßnahmen, die in der aktualisierten Version 2022 der Norm auf 93 Maßnahmen mit vier Hauptmaßnahmenkategorien umstrukturiert wurden. Die Aktualisierung umfasste auch 11 neu hinzugefügte Maßnahmen. Insgesamt sollen diese verschiedenen Maßnahmengruppen einer Organisation helfen, ihre Informationssicherheit zu verbessern. Die ISO/IEC 27002 enthält detaillierte Erläuterungen zu jeder Maßnahmenkategorie und deren Maßnahmen, einschließlich der wichtigsten Ziele und Vorgaben.

Die Entscheidung, welche Maßnahmen in einer Organisation umgesetzt werden und welche nicht, obliegt der Organisation, sofern diese Entscheidungen in einer SoA dokumentiert werden.

Die Wirksamkeit der umgesetzten Maßnahmen kann auf unterschiedliche Weise gemessen werden. Entscheidend ist dabei aber, dass sie zur Risikomanagementstrategie des ISMS beitragen.